microWIU™

WARNING

This is a Vital product. Any changes may compromise the safe performance of this unit.

Operation and Maintenance Manual
P2525

microWIU™

WARNING

This is a Vital product. Any changes may compromise the safe performance of this unit.

Operation and Maintenance Manual

Alstom Signaling Inc.

P2525, Rev. E, October 2013, Printed in U.S.A.

LIST OF EFFECTIVE PAGES

P2525, microWIU™ Operation and Maintenance Manual

ORIGINAL ISSUE DATE: June 2012

CURRENT REVISION AND DATE: Rev E, October 2013

PAGE	CHANGE OR REVISION LEVEL
Cover	Oct/13
Title page	Oct/13
Preface	Oct/13
i through iv	Oct/13
1–1 through 1–20	Oct/13
2–1 through 2–8	Oct/13
3–1 through 3–22	Oct/13
4–1 through 4–28	Oct/13
5–1 through 5–16	Oct/13
6–1 through 6–2	Oct/13
7–1 through 7–4	Oct/13
8–1 through 8–4	Oct/13
A–1 through A–6	Oct/13
B–1 through B–2	Oct/13
C–1 through C–10	Oct/13

THIS PAGE INTENTIONALLY LEFT BLANK.

PREFACE

NOTICE OF CONFIDENTIAL INFORMATION

FOR QUESTIONS AND INQUIRIES, CONTACT CUSTOMER SERVICE AT
1–800–717–4477
OR
WWW.ALSTOMSIGNALINGSOLUTIONS.COM

ALSTOM SIGNALING INC
1025 JOHN STREET
WEST HENRIETTA, NY 14586

REVISION LOG

Revision	Date	Description	By	Checked	Approved
1(A)	June 2012	Original Issue	LR	EK	NI
2(B)	June 2012	Note added in Section 4; Circuit drawings added in Appendix A	LR	EK	NI
3(C)	September 2012	Changes on page A-7	LR	EK	NI
D	April 2013	Updated for enhancements	SG	EK	NI
E	October 2013	Updated warning / caution statements; added descriptions in Appendix	SG	EK	MS

THIS PAGE INTENTIONALLY LEFT BLANK.

ABOUT THE MANUAL

This manual is intended to provide the necessary information to maintain and ensure the proper operation of the Alstom microWIU™.

The information in this manual is arranged into sections. The title and a brief description of each section follow:

Section 1 – GENERAL DESCRIPTION: This section provides general information about the components of the Alstom microWIU.

Section 2 – THEORY OF OPERATION: This section provides general information about the functional operation of the Alstom microWIU.

Section 3 – INSTALLATION: This section describes the field installation and setup of the Alstom microWIU.

Section 4 – OPERATION: This section provides instructions on using the Alstom microWIU.

Section 5 – SOFTWARE UPDATES: This section provides instructions for updating the application software for the Alstom microWIU.

Section 6 – TROUBLESHOOTING: This section describes possible failures/symptoms along with the corrective action for the Alstom microWIU.

Section 7 – CORRECTIVE MAINTENANCE: This section describes the corrective maintenance of the Alstom microWIU.

Section 8 – PARTS CATALOG: This section identifies and lists the spare parts associated with the Alstom microWIU.

Appendix A – TYPICAL APPLICATION CIRCUITS: This section provides examples of typical Alstom microWIU application circuits.

Appendix B – PREPARATION PROCESS DATA SHEET: This section provides the validation data sheet.

Appendix C – SAFETY-RELATED APPLICATION CONDITIONS / ACTIONS: This section contains the Safety-Related Application checklist to record all evidence required by the customer/railroad to validate information contained in the microWIU application before beginning revenue service.

THIS PAGE INTENTIONALLY LEFT BLANK.

MANUAL SPECIAL NOTATIONS

In the Alstom manuals, three methods are used to convey special informational notations. These notations are warnings, cautions, and notes. Both warnings and cautions are readily noticeable by boldface type and a box around the entire informational statement.

Warning

A warning is the most important notation to heed. A warning is used to tell the reader that special attention needs to be paid to the message because if the instructions or advice is not followed when working on the equipment then the result could be either serious harm or death. The sudden, unexpected operation of a switch machine, for example, or the technician contacting the third rail could lead to personal injury or death. An example of a typical warning notice is:

WARNING

Disconnect the motor energy whenever the gear cover is removed. Otherwise, the switch machine may operate unexpectedly and possibly cause personal injury.

Caution

A caution statement is used when an operating or maintenance procedure, practice, condition, or statement, which if not strictly adhered to, could result in damage to or destruction of equipment. A typical caution found in a manual is:

CAUTION

Turn power off before attempting to remove or insert circuit boards into a module. Boards can be damaged if electrical power is not turned off.

Note

A note is normally used to provide minor additional information to the reader to explain the reason for a given step in a test procedure or to just provide a background detail. An example of the use of a note is:

Note: Leads must be long enough to allow strain relief, thus eliminating local tension.

THIS PAGE INTENTIONALLY LEFT BLANK.

TABLE OF CONTENTS

Topic **Page**

TABLE OF CONTENTS

Topic **Page**

LIST OF FIGURES

LIST OF TABLES

SECTION 1 – GENERAL DESCRIPTION

1.1 SAFETY WARNINGS AND CAUTIONS

WARNING

This is a Vital product. Any changes may compromise the safe performance of this unit.

WARNING

The microWIU Vital input circuits may activate with a minimum signal of 3.4 V and 10.2 milliamperes in worst case scenario under failure conditions.

To prevent a potential unsafe condition, any external voltage source attached to a microWIU Vital input circuit must generate less than 3.4 V and 10.2 milliamperes in worst case scenario under failure conditions when the device controlling the source voltage is in the de-energized state.

This requirement includes all environmental operating conditions and all operating values of the external voltage source over its service life, including worst case scenario under failure conditions. Failure to follow this requirement may lead to unexpected operation of the microWIU input circuit.

WARNING

The microWIU Vital input circuits may fail with a complete short between the input positive and negative terminals. To prevent a potential unsafe condition, this failure mode must be considered when the microWIU Vital input circuit is connected in parallel with any other load device (e.g., a signal lamp).

This requirement includes all environmental operating conditions and all operating values of the load device over its service life. Failure to follow this requirement may lead to unexpected operation of the microWIU input circuit.

WARNING

Prior to software installation, validation testing must confirm all application logic is correct and consistent with application requirements.

WARNING

Before using an Application generated by the ADT, the user must execute the procedure described in P2526 ADT User Manual SECTION 6 – Application Data Verification to ensure Vital application data structures are correct.

WARNING

It is the responsibility of the railroad to ensure personnel are thoroughly trained and sufficiently knowledgeable regarding safety requirements and precautions affecting the microWIU system performance.

WARNING

It is the responsibility of the railroad to ensure formal application engineering training to explain proper selection and use of VSOE2, including, but not limited to, message configuration.

WARNING

Certain replacement hardware is identified by unique keying of input connectors. Proper care needs to be given to ensure keying of new connectors matches those being replaced.

WARNING

Field testing of an Application is required before placing the location into revenue service. The customer's testing plan and safety plan define the testing requirements for the Application.

WARNING

Railroad correspondence (validation) testing must be conducted to ensure that microWIU configuration and physical connections agree with railroad track conditions.

WARNING

Railroad personnel, using the verification and validation process, must ensure that the microWIU is programmed with the correct application logic and consistent with application requirements.

WARNING

Railroad personnel, using the verification and validation process, must ensure that the microWIU is correctly configured.

WARNING

Personnel must be trained and qualified, in accordance with the product installation or maintenance manuals, before installing or servicing microWIU equipment.

WARNING

It is the railroad’s responsibility to ensure remote access via a TCP/IP connection is secured and controlled by a passcode.

WARNING

It is the railroad’s responsibility to establish and maintain the Security Levels through the ADT for microWIU window access. Restriction of unauthorized personnel to functions that can affect safety is imperative.

WARNING

Proper PTC operation must be verified by field test before use and after any repair.

WARNING

Product manuals clearly define all maintenance requirements of the system, and training must be sufficient to convey understanding of safety requirements.

WARNING

Use of the Application Development Tool must be limited to only skilled and trained application designers (application engineers).

WARNING

The microWIU must never be opened and/or serviced by anyone other than Alstom.

CAUTION

Applications created with a previous version of ADT software (i.e., different than the microWIU is currently running) need to be recompiled with the version of ADT software that matches the version on the target microWIU. Applications compiled in an older ADT version will render the microWIU nonfunctional.

CAUTION

Maintainers must review microWIU error logs and repair or remove a microWIU from service within four days of reported failure:

- Heath-Sync-Lost
- Fatal-Error type error(s)
- Any microWIU reported as potentially impacting operations

CAUTION

Any operational impact that may be due to the microWIU (such as, On-Board unit fails to receive message from microWIU or On-board unit receives invalid messages from the microWIU) must be reported to the maintenance department daily by railroad personnel (i.e., locomotive engineers or trackside workers).

1.2 INTRODUCTION

This section provides a general description of the Alstom microWIU™.

1.3 ABBREVIATIONS AND ACRONYMS

See Table 1–1 for a list of the abbreviations and acronyms used throughout this manual.

Table 1–1. Terminology

Term	Definition
AAR	Association of American Railroads
ACSES	Advanced Civil Speed Enforcement System
ADT	Application Development Tool
ADV	Application Data Verifier
AREMA	American Railway Engineering and Maintenance-of-Way Association
ASES	US&S PTC system
ATCS	Advanced Train Control System
AWG	American Wire Gage
BL	Baseline
BOP	Book of Plans
CAN	Controller Area Network
CRC	Cyclic Redundancy Check
EMP	Edge Message Protocol
FRA	Federal Railroad Administration
HMAC	Hash-based Message Authentication Code
I/O	Input/Output
IP	Internet Protocol
ITC	Interoperable Train Control
LED	Light Emitting Diode
LoMA	Limit of Movement Authority
LRU	Lowest Replaceable Unit
NISAL	Numerically Integrated Safety Assurance Logic
NoLoMA	No Limit of Movement Authority
NTP	Network Time Protocol
NVP	Non-Vital Processor

Table 1–1. Terminology (Cont.)

Term	Definition
OBC	On-board Computer
POSIX	Portable Operating System Interface for Unix
PTC	Positive Train Control
ROM	Read-Only Memory
TCP	Transmission Control Protocol
TRM	Train Request Message
TTL	Time to Live
UDP	User Datagram Protocol
USB	Universal Serial Bus
VDC	Volts Direct Current
V-ETMS	Vital Electronic Train Management System
VSOE	Vital Serial Over Ethernet
WEU	Wayside Encoder Unit
WIU	Wayside Interface Unit
WMS	Wayside Management Server
WSM	Wayside Status Message

1.4 GENERAL

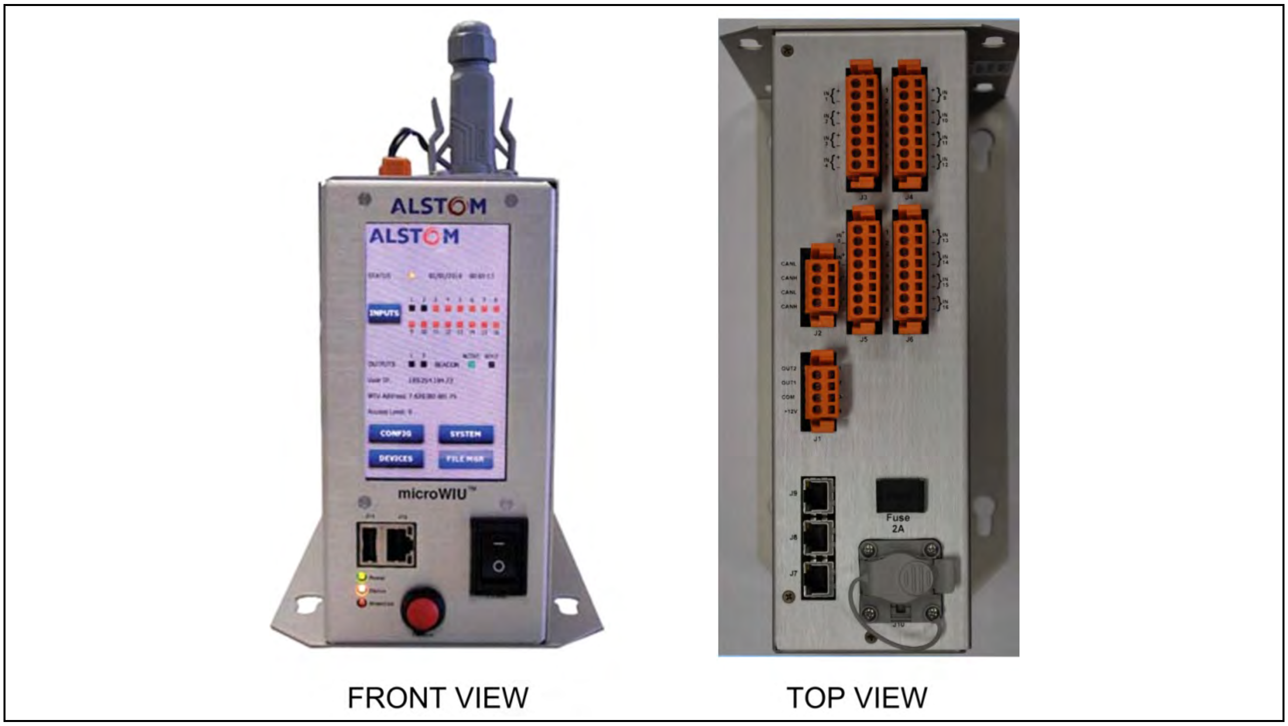
The microWIU product is a standalone Wayside Interface Unit (WIU) designed to address the Positive Train Control (PTC) initiative mandated by the Federal Railroad Administration (FRA). The PTC mandate does not prescribe a particular system solution to implement the requirement, and multiple solutions or standards are used across the industry. The WIU function is required for all PTC implementations to provide the link between conventional wayside signaling devices and the signaling communication network.

The microWIU supports two PTC system standards that are being utilized by various U.S. railroads:

1. The Interoperable Train Control (ITC) standard developed by the American Association of Railroads (AAR), and
2. The Advanced Civil Speed Enforcement System (ACSES), originally developed by Alstom for Amtrak

For both PTC standards, the WIU function monitors the state of wayside signaling equipment (signals, switches) and provides this information via a PTC data network to an approaching train, whose on-board computer (OBC) uses this information to enforce safe operation of the train.

The microWIU is available in two front panel configurations: with and without a power switch.



FRONT VIEW

TOP VIEW

Figure 1-1. MicroWIU with Power Switch, Front and Top Views

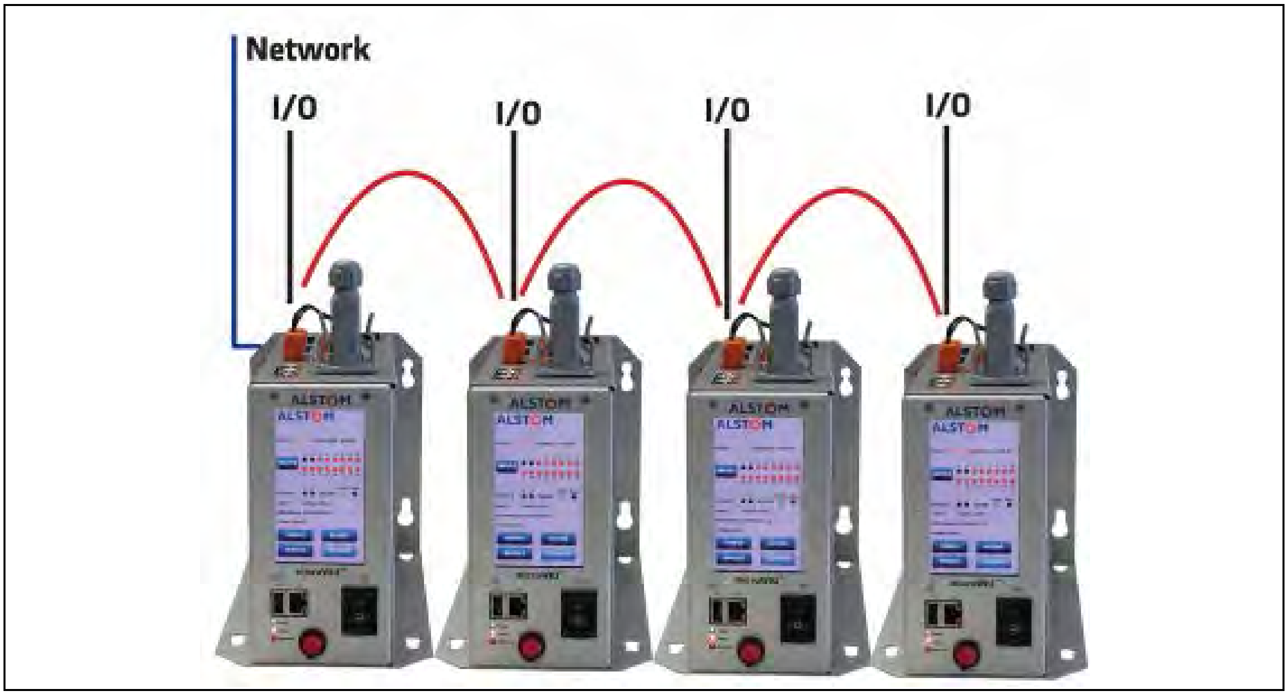


Figure 1-2. Stacked microWIU Configuration (Master and Three Slaves)

1.5 FEATURES

The Alstom microWIU provides:

- Features that meet ACSES and AAR ITC WIU specifications
- Stackable to seven units with small footprints for input/output (I/O) expansion
- Expandable up to 1500 ft., (with a 2 or 3 slave configuration), limiting inputs to 43 and outputs to 3
- Low-power design for solar/alternative energy compatibility
- A built in auto power-save feature that further conserves power during inactive times
- All units operate from a standard 12 VDC signal battery
- 16 Vital digital inputs and 2 non-vital outputs per unit
  - A total of 112 Vital inputs and 14 non-vital outputs
- Emergency Vehicle Preemption Class C/D protocols for ITC
- Local and remote configuration and monitoring
  - Using the integrated color touch-screen display, installation and maintenance can be performed efficiently without a computer, but the unit may also be configured, managed and monitored either locally or remotely over Ethernet, facilitated by its embedded web server
- User-friendly Application Development Tool (ADT) for defining application configurations
- Transmission Control Protocol/User Datagram Protocol/Internet Protocol (TCP/UDP/IP)
- Integrated web server provides parallel status and configuration capabilities
- Embedded Data Logging
- Integrated Temperature Alarm/Monitoring
- Built-in Status/Report Generator
- Site configuration stored on a USB device located on top of the unit in a protective housing
  - No special hardware is needed to program the plug since it is compatible with commonly available computer equipment
- Support for up to eight legacy ACSES Wayside Encoder Unit (WEU) addresses
- Vital inputs support voltage and optional external current sensing detection
- Simultaneous support for V-ETMS and ASES II protocols
- Requires no periodic or preventive maintenance

1.6 COMPONENTS

The microWIU is a single, line-replaceable unit housed in a sheet metal enclosure. The touch screen display is mounted on the front of the unit, along with a network port and USB port. The balance of the network ports, an additional USB port, Controller Area Network (CAN) connections, and Vital input and non-vital output connections are located on the top of the unit. The unit is powered from a 10–16.5 VDC source, and can be mounted on a wall, shelf, or 19-inch rack (using a B2- or B3-width relay adapter plate).

The microWIU includes the following visible components:

- Integrated color touch screen display:
  - Acts as the configuration and status interface for installation, operation, and maintenance
  - Provides status and configuration access without a laptop
- Discrete LEDs provide power/health indication when the touch screen is in power saving mode (touch to activate)
- Front panel USB port for user upload and download of software components and Maintenance Logs
- Four Ethernet Ports:
  - Front panel Ethernet port for user web-server access for status and configuration (same as touch screen), and ITC simulator
  - Two Ethernet ports for independent PTC network communication paths capable of being configured as different subnets (ACSES and ITC)
  - One Ethernet port for master/slave network configuration or VSOE2 (local only)
- Heavy-duty USB device (located on top of the microWIU)

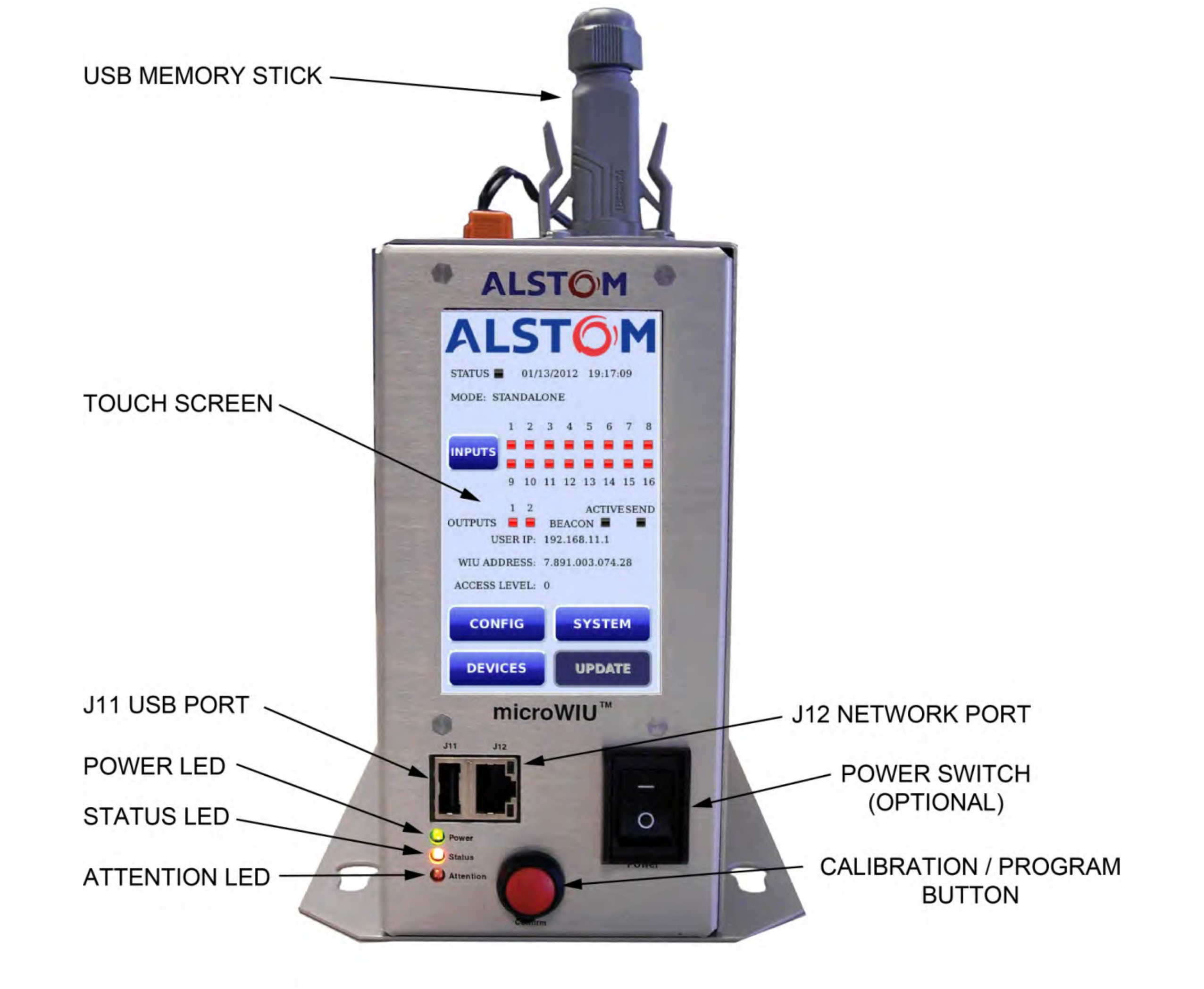


Figure 1-3. microWIU Front View Detail

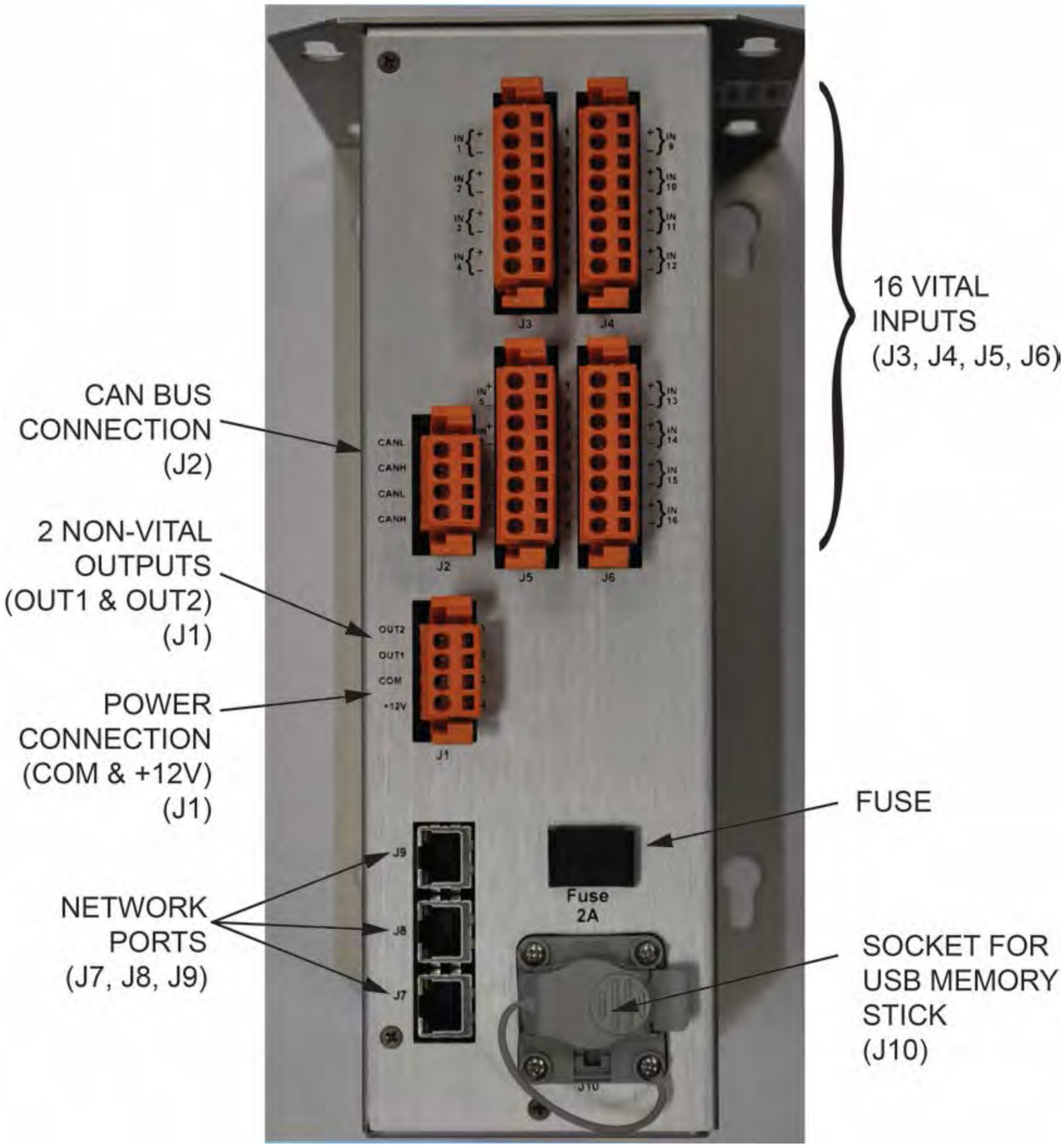


Figure 1-4. microWIU Top View Detail

The microWIU system can be divided into several architectural components:

- Display Controller: The Display Controller interfaces with a standard low-level protocol to the touch screen for graphics display and touch screen input control; the display controller has a high-speed serial data interface to the Non-Vital Processor section
- Non-Vital Processor (NVP) Section: The NVP section controls the majority of the non-vital functions of the microWIU including network protocols, USB file system, controls and displays, and the non-vital communications protocol layers
- Vital Processor Section: The Vital Processor section:
    - Controls and monitors the Vital input circuits and controls the non-vital outputs
    - Implements a CAN interface to other microWIU units if a master/slave configuration is used for an application
    - Executes Vital Boolean equations using Numerically Integrated Safety Assurance Logic (NISAL) safety techniques
    - Implements the Vital Serial Over Ethernet (VSOE2) protocol if a VSOE communication link is defined for an application
    - Generates Vital PTC output messages for ACSES (if enabled) based on the user-defined application data and the state of the Vital inputs
    - Generates Vital PTC output messages for the ITC operating mode (if enabled)
- Vital Input Circuits: 16 identical, isolated Vital input circuits are available for interfacing to wayside devices; these are controlled and monitored by the Vital Processor section through a parallel data interface
- Non-vital Outputs: Two non-vital outputs are available to drive approach lighting relays

1.7 SPECIFICATIONS

The microWIU meets or exceeds the environmental parameters as set forth in AREMA Manual Part 11.5.1 for Class C equipment.

- Power Supply: 10 VDC to 16.5 VDC @ 1 amp
- Operating Temperature: –40 °C to +70 °C (–40 °F to +158 °F)
- Storage Temperature: –55 °C to +85° C (–67 °F to +185 °F)
- Humidity: 0 to 95% non-condensing
- Vital Isolation (input-to-input and input-to-earth): 3000 VAC
- Weight: 3.5 lbs
- Vital Inputs:
  - ON State: 8 VDC to 16.5 VDC, 9 VAC RMS to 16 VAC RMS
  - OFF State: 0 VDC to 3 VDC, 0 VAC RMS to 2 VAC RMS
  - Maximum Withstand: 18 VDC
- Non-vital Outputs: 12 VDC nominal, 100 Ω to 2000 Ω load

1.8 DIMENSIONS

- The microWIU unit measures 3.5 in. wide x 7 in. high x 11 in. deep (8.9 cm w x 17.8 cm h x 27.9 cm d)
  - With the USB device inserted, the microWIU measures 10 in. high (25.4 cm)
- With the standard B-3 mounting flange attached, the unit measures 5.5 in. wide x 7 in. high x 11 in. deep (14 cm w x 17.8 cm h x 27.9 cm d)
- A smaller microWIU mounting plate (B2-width flange) is available measuring 5.0 in. wide x 7 in. high x 11 in. deep (12.7 cm w x 17.8 cm h x 27.9 cm d)

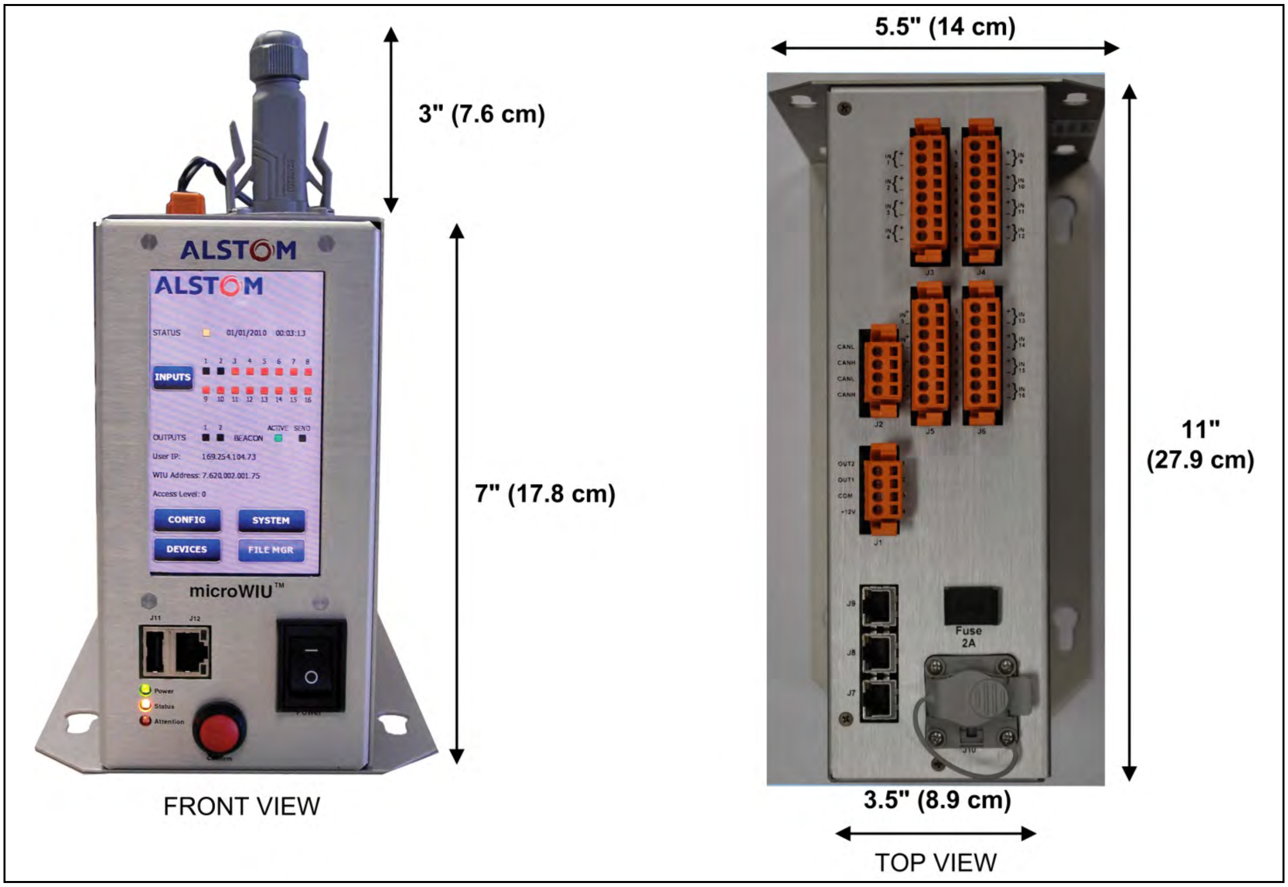


Figure 1-5. MicroWIU Dimensions with B3 Flange

1.9 APPLICATIONS

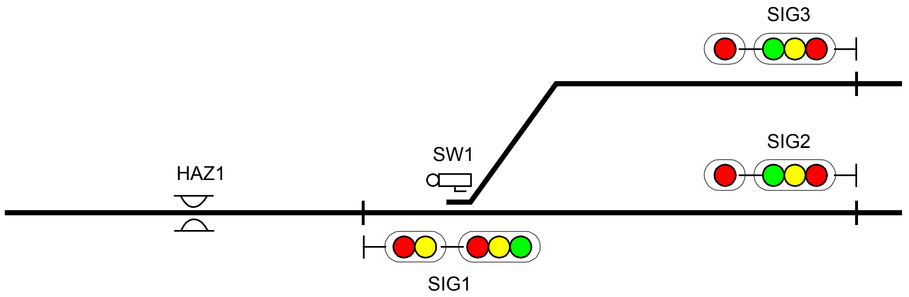
The microWIU supports the following applications:

- Small-to-medium scale overlay of existing signaling locations or can be expanded to support large locations by stacking the units
- Hand Throw Switch and Hazard (such as a slide fence) monitoring in dark territory
- Interconnection of up to seven microWIU units (one master and six slaves)
- Four IP ports:
  - One user port or embedded web server
  - Two ports for ITC and ACSES network
  - One port for master/slave IP network or VSOE2 connection

To determine how many microWIU units are required for a location, use the ADT (Application Development Tool), or follow the steps in Table 1–2.

Table 1–2. Determining the Required Number of microWIU Units for a Location

Step	Procedure
1	Determine the number and type of devices for a location (switches, signals, and hazard detectors).
2	Determine the total number of physical inputs required by adding the number of inputs per device. If the total is over 16, more than one microWIU is required (stacked configuration). The number of units required is total number of inputs required divided by 16, then rounded up to next whole number.
3	For ITC configuration, use the ADT to map physical devices to device codes: • Hazard Detectors: Single bit, no mapping required • Switches: User assigns Normal and Reverse inputs • Signals: User defines signal configuration (codes mapped from railroad-specific aspect table)



Sample Input Mapping

Input	Signal
1	SW1N
2	SW1R
3	SIG1AR
4	SIG1AY
5	SIG1AG
6	SIG1BR
7	SIG1BY
8	HAZ1

Input	Signal
9	SIG2AR
10	SIG2BR
11	SIG2BY
12	SIG2BG
13	SIG3AR
14	SIG3BR
15	SIG3BY
16	SIG3BG

Sample Aspect Table

Signal Aspect	Device Code
G/R	3 (00011)
FY/R	6 (00110)
Y/R	8 (01000)
R/Y	12 (01100)
R/FR	13 (01101)
R/R	15 (01111)
Invalid	31 (11111)

Figure 1-6. Example microWIU ITC Application Information

Figure 1-7 shows a typical standalone ITC configuration.

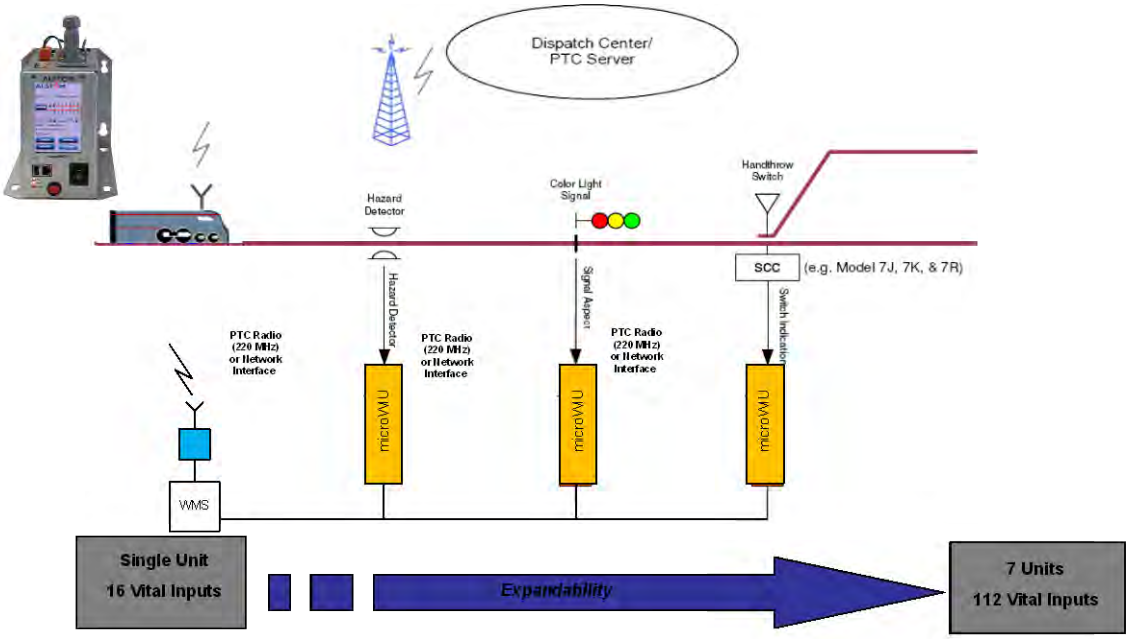


Figure 1-7. Typical Application – Standalone (Small Overlay Application) microWIU

1.10 ITC CONFIGURATION

Figure 1-8 shows the architecture of overall PTC system when configured for the ITC application. The microWIU is applicable to the Wayside Interface Unit (WIU) portion of the system.

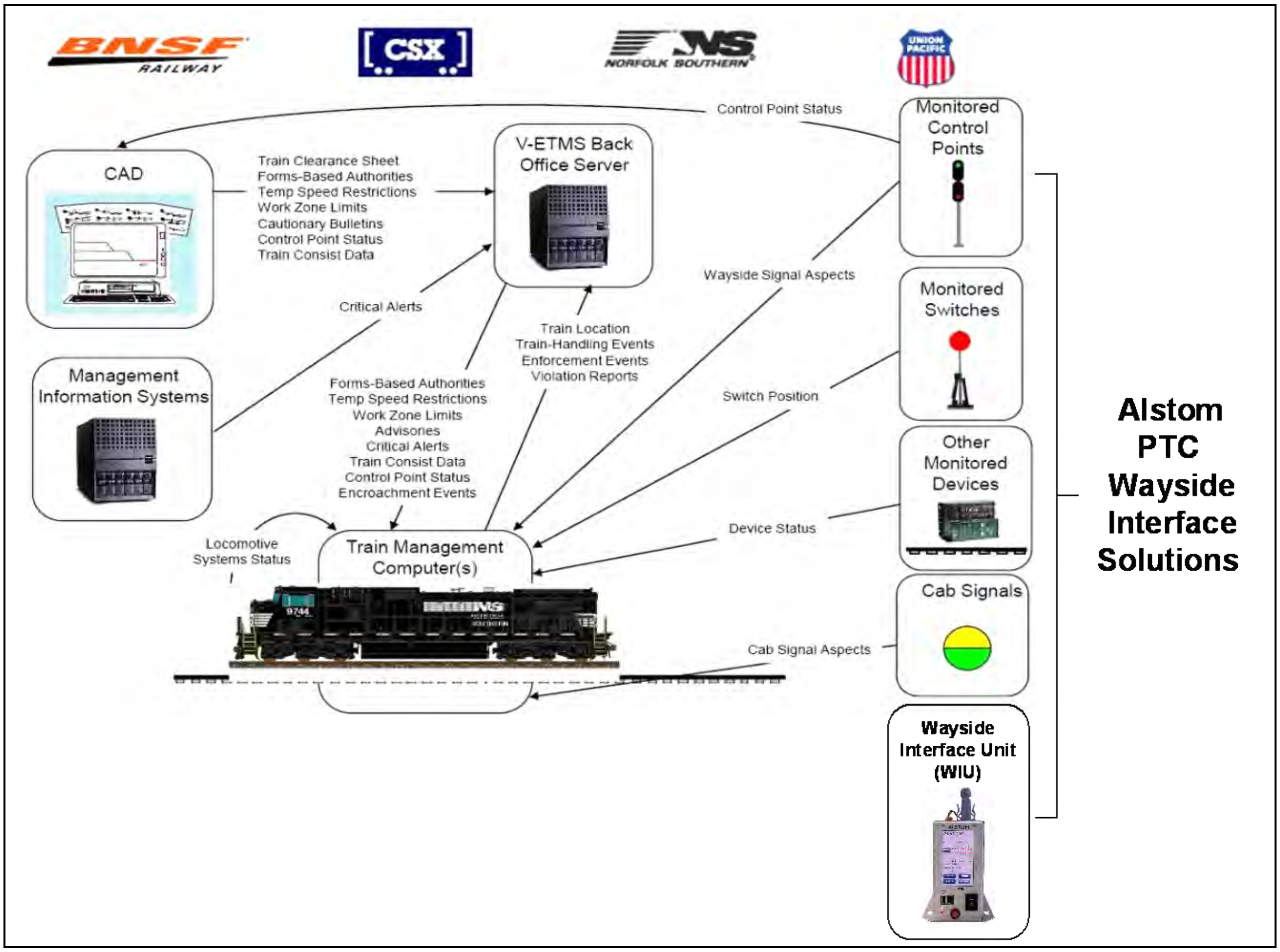


Figure 1-8. Example ITC Configuration

1.11 ACSES CONFIGURATION

Figure 1-9 shows the architecture of overall PTC system when configured for the ACSES application. The microWIU is applicable to the Wayside Interface Unit (WIU) portion of the system.

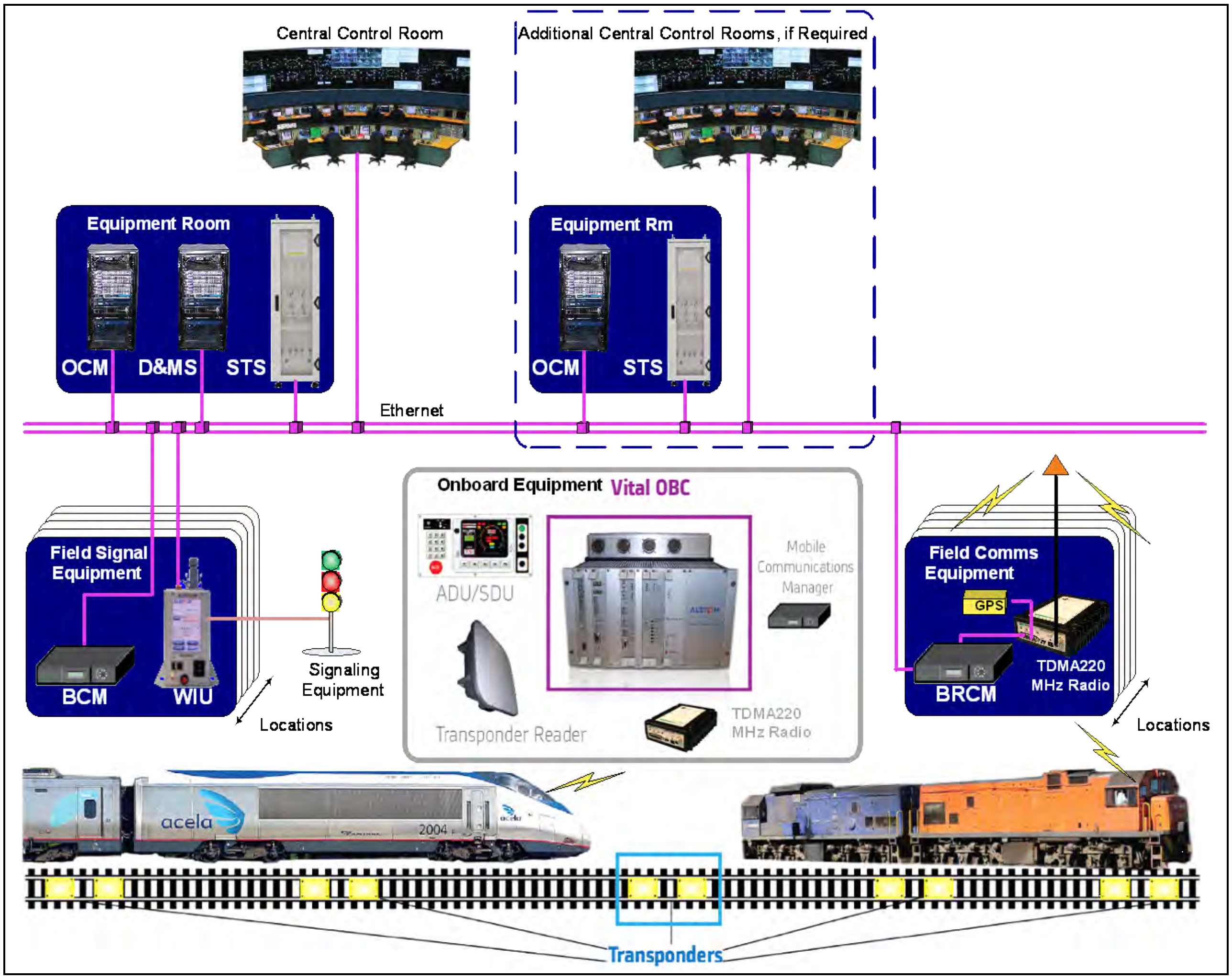


Figure 1-9. Example ACSES Configuration

THIS PAGE INTENTIONALLY LEFT BLANK.

SECTION 2 – THEORY OF OPERATION

2.1 GENERAL

This section contains a functional description of the microWIU.

WARNING

It is the responsibility of the railroad to ensure personnel are thoroughly trained and sufficiently knowledgeable regarding safety requirements and precautions affecting the microWIU system performance.

2.2 INTRODUCTION

The Alstom microWIU performs the following internal functions:

- Monitor System Inputs: Monitors the WIU's Vital hardware inputs
- Prepare System Outputs: For each operating mode, creates/selects PTC message outputs per current system inputs and updates non-vital hardware output states
- Manage PTC Networks: Monitors configured Ethernet interface(s) for incoming PTC network messages, processes messages, routes incoming messages, and routes outgoing PTC network messages to configured Ethernet interface(s) for transmission
- Internal System Management: Executes system cycle, updates displays, and performs background diagnostic monitoring and logging of system operational events
- Manage User Interaction: Asynchronous user interaction for status queries and configuration actions
- Manage Off-line Tasks: This function manages system tasks such as software/firmware updates, encryption key updates
- ITC Test Mode: Test feature to inject simulated ITC train request messages and view content of the reply messages
- Shadow Mode: Shadow Mode is available only when the microWIU is used in ACSES Mode. When in Shadow Mode, the microWIU sends messages to an IP address as specified in the ADT instead of sending messages to the train. The microWIU vitally ensures that messages accidentally sent to the train through the existing active radio link are not processed by the on-board computer
  - Shadow Mode is enabled only through the ADT

2.3 VITAL SYSTEM CYCLE

The microWIU Vital I/O Processor executes a one-second system cycle during which Vital inputs are read, input parameters updated, Vital equations executed, and Vital result parameters and non-vital outputs updated. These operations are common in all PTC operating modes.

WARNING

Proper PTC operation must be verified by field test before use and after any repair.

CAUTION

Maintainers must review microWIU error logs and repair or remove a microWIU from service within four days of reported failure:

- Heath-Sync-Lost
- Fatal-Error type error(s)
- Any microWIU reported as potentially impacting operations

CAUTION

Product manuals clearly define all maintenance requirements of the system, and training must be sufficient to convey understanding of safety requirements.

CAUTION

Any operational impact that may be due to the microWIU (such as, On-Board unit fails to receive message from microWIU or On-board unit receives invalid messages from the microWIU) must be reported to the maintenance department daily by railroad personnel (i.e., locomotive engineers or trackside workers).

2.3.1 Vital Inputs

Input state detection is performed on a one-second cycle for all inputs, with each input result provided to the system cycle as OFF, ON, or Flashing.

> Note: If flash state detection is enabled, the allowable flash rate range of 35 ppm–75 ppm is used.

2.3.2 Vital Boolean Parameters

A set of Vital Boolean parameters is maintained by the Vital Processor section using 32-bit codeword representations for Vital parameters. They are updated by a combination of Vital input processes (Vital hardware reads and Vital data protocol decoding) and Vital equation evaluation. Vital parameters are evaluated and updated every system cycle.

ACSES messages are vitally selected by their respective unique set of Vital input parameter states defined by the Application Program.

ITC Device Code bits are represented by Vital parameters that are calculated based on Vital logic determined by:

- For signals, the logic defined by the Aspect Table
- For switches, the inputs defined to represent normal and reverse states
- For hazard detectors (such as generic single inputs), the single input state

2.3.3 System Health Verification

The system cycle on the microWIU includes a process to validate the underlying operation of the system, including cycle timing, ROM integrity, and Vital memory management.

2.3.4 Vital Data Protocol

A Vital Serial Over Ethernet (VSOE2) protocol implementation provides Vital input parameters from other Alstom systems (such as VPI, iVPI) to the microWIU. The Vital data protocol process directly updates the Vital parameter buffer each system cycle.

2.4 COMMUNICATION

2.4.1 WIU – ACSES Communications

The microWIU generates four Vital output message types for ACSES:

1. Type 22 (Home Signal Status Response with LoMA)
2. Type 23 (Home Signal Status Response without LoMA)
3. Type 25 (Intermediate Signal Status Response with LoMA)
4. Type 26 (Intermediate Signal Status Response without LoMA)

One of these message types is always generated in response to a Type 21 (Train Request Message) message. The Vital message protocol used for the Vital output messages is a form of Vital ATCS that consists of a 72-bit CRC of the first 183 bits of the output message data payloads.

A set of output messages is defined by the application programmer for a given location. The proper message to transmit in response to a Train Request Message (TRM) is a function of the following:

1. State of Vital inputs (switch positions, signal GO states)
2. The particular home signal status requested

Two fields in the 183-bit data block of a stored message are overwritten by the data received in the TRM: the pseudo-random time stamp and the train ID. These values are echoed back to the requesting train to provide an indication that the message is in response to the proper request.

In normal operation, the microWIU responds to a Type 21 message (TRM) by retrieving the proper stored message based on the following:

- WIU Address
- Requested Signal
- Vital input states (switch and signal status); if a valid message is retrieved, the message is then assembled and sent to the train

If a valid message is not found, a Type 24 message (Error Response Message) is generated. While this message is functionally non-vital, it is also protected by a 72-bit CRC.

2.4.2 WIU – ITC Communications

The ITC WIU standard has a single Vital output message format: the Wayside Status Message (WSM). Unlike ACSES, with a pre-defined set of messages indexed by input conditions, the ITC standard defines wayside device types whose individual status is conveyed to any trains in the area. The ITC OBC is responsible for interpreting how the status for individual devices affects their authorized speed or limit of authority. The three ITC-defined device types are:

1. Hazard Detector (such as a slide fence, dragging equipment detector, etc.): State represented by 1 bit in the WSM
2. Switch: Represented by 2 bits in the WSM (1 bit each for Normal and Reverse indications from a hand throw switch)
3. Signal: Composite aspect code represented by 5 bits in WSM (assignments from railroad-specific aspect tables); bit values determined from Boolean equations driven by signal displaying states

A given WSM may have multiple devices of each device type depending on the layout of the location. For the most basic Hand Throw Switch monitoring application, the WSM may contain just a single switch device.

The Vital message protocol used for the WSM is the Keyed-Hash Message Authentication Code (HMAC) using a truncated SHA-1 algorithm (128-bit message digest truncated to 32-bits). This is defined by the U.S. National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication 180-2.

The WSM is transmitted both in response to a specific request from a train, and autonomously based on a user-defined transmission rate or optionally on any input state change. Unlike the ACSES output messages, the WSM does not contain data intended for a single train, but broadcasts the same wayside status information to all trains in the area.

Because the number and type of wayside devices at a given location are variable, the WSM Vital message size is also variable. Not all of the fields in the message payload are functionally Vital, but all of the message payload bits are used in the HMAC calculation, along with two fields that are not transmitted in the message, but maintained separately by the WIU and the OBC (POSIX time and Config CRC). These values must be in correspondence between the WIU and the OBC for Vital message validation to be possible.

2.5 LEDS

Three LEDs on the front of the microWIU quickly verify unit performance. See Figure 2–1 and Table 2–1 for more information.

When the touch screen is in power-save mode, only the Power and Status LEDs are active.

During the microWIU power-up sequence, the Status and Attention LEDs flash GREEN until the boot process is complete.

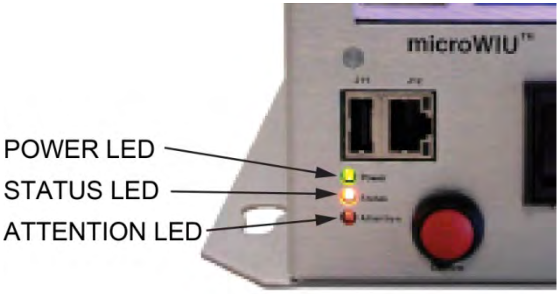


Figure 2-1. Location of Front Panel LEDs

Table 2–1. LED Functions

LED	Function
Power	GREEN when the microWIU is powered
Status	• GREEN when the unit is operating normally (no warnings) • YELLOW when a warning condition has been detected, but the unit is operating (possibly in a degraded mode depending on the warning condition) • RED when an error condition has been detected and the unit is not operational
Attention	RED when a condition exists that requires user attention

2.6 APPLICATION PROGRAMMING OVERVIEW

The application programmer uses the ADT and a separate application data verifier (ADV) to generate the application file set used by the microWIU to implement the desired functionality.

The application file set is transferred to the microWIU using a USB device. The microWIU reads the application file set provided and uses its pre-programmed system (executive) software to execute the PTC functions of the defined PTC mode(s). At a high level, the PTC functions implemented by the unit are described as follows:

- ACSES:
  - Monitor Vital inputs
  - Manage Train Request Messages
  - Select appropriate status messages
  - Select Vital Output Message (LoMA, NoLoMA, Error)
  - Manage user interfaces (local and remote)
  - Manage remote systems management functions
- ITC:
  - Monitor Vital inputs
  - Assemble ITC device codes
  - Build Wayside Status Message (WSM)
  - Manage EMP Class C time updates
  - Manage NTP time updates
  - Manage EMP Class D Beacon messages
  - Manage ITC Beacon timing
  - Manage user interfaces (local and remote)
  - Manage remote systems management functions

The normal operating modes of the microWIU are ACSES and ITC. Applications are configured with the ADT to support either operating mode.

THIS PAGE INTENTIONALLY LEFT BLANK.

SECTION 3 – INSTALLATION

3.1 GENERAL

This section contains general installation procedures for the microWIU. Included is a procedure for inspecting each unit prior to installation, followed by the installation and configuration procedure.

WARNING

It is the responsibility of the railroad to ensure personnel are thoroughly trained and sufficiently knowledgeable regarding safety requirements and precautions affecting the microWIU system performance.

3.2 HARDWARE INSTALLATION

The microWIU can be mounted on a wall, shelf, or 19-inch rack (using a B2- or B3-width flange).

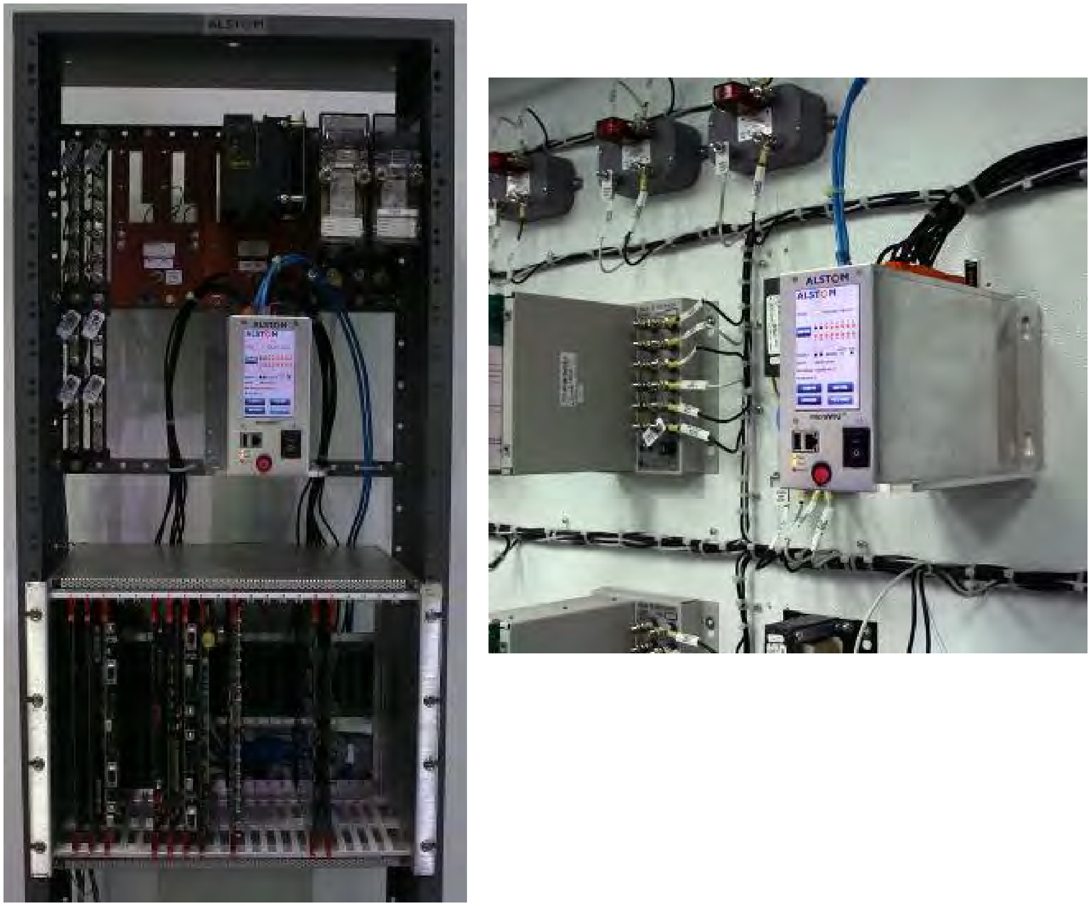


Figure 3-1. Rack and Wall Example Mounting

The procedure in Table 3–1 provides an overview of how to install the microWIU at a new site. See the site-specific Book of Plans (BOP) for mounting and wiring details for the specific configuration.

Table 3–1. microWIU Installation Procedure

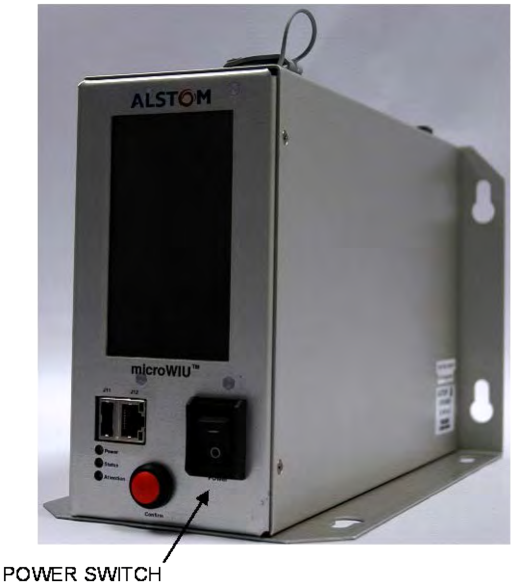
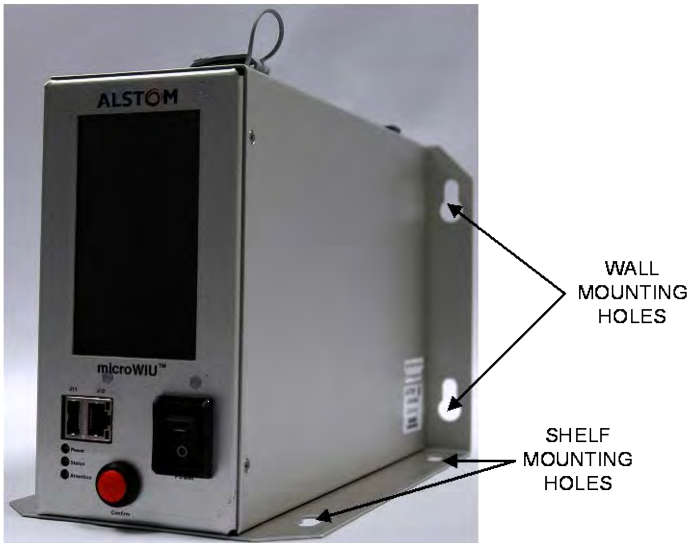
Step	Procedure
1	Verify that the power to the power cable is disconnected.
2	Verify the microWIU power switch is in the OFF position, if applicable. 
3	Using the mounting holes provided on the unit, install the appropriate mounting hardware. See the site-specific Book of Plans as required. 

Table 3–1. microWIU Installation Procedure (Cont.)

Step	Procedure
4	Connect power, input, output, and data cables as specified in the site-specific Book of Plans.
5	Supply power to the unit. See the site-specific Book of Plans as required.
6	Turn the unit power switch to the ON position, if applicable. The Power and Status LEDs flash during the microWIU boot process.

3.3 SOFTWARE INSTALLATION

Refer to Appendix B and Appendix C for additional application data details.

3.3.1 Local Software Installation

WARNING

Prior to software installation, validation testing must confirm all application logic is correct and consistent with application requirements.

WARNING

Before using an Application generated by the ADT, the user must execute the procedure described in P2526 ADT User Manual SECTION 6 – Application Data Verification to ensure Vital application data structures are correct.

CAUTION

Applications created with a previous version of ADT software (i.e., different than the microWIU is currently running) need to be recompiled with the version of ADT software that matches the version on the target microWIU. Applications compiled in an older ADT version will render the microWIU nonfunctional.

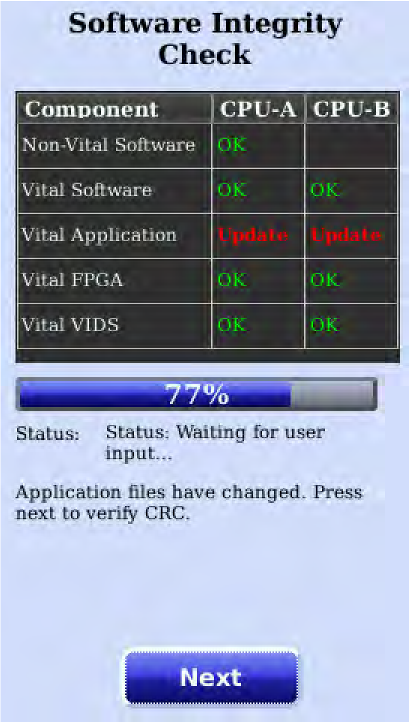
When a USB device is initially inserted into the top USB port of the microWIU, the unit begins the installation process of loading the application and operating system software.

See Table 3-2 for the software installation procedure.

Table 3-2. Local Software Installation Procedure

Step	Procedure
1	Verify the USB device’s label is consistent with the correct site-specific application for transfer onto the microWIU.
2	Record results on Table B-1, Line 2.

Table 3-2. Local Software Installation Procedure (Cont.)

<table>
<tr><th>Step</th><th>Procedure</th></tr>
<tr><td>3</td><td>Insert the programmed USB device into the top USB port.
Note: A programmed USB device is required in the top USB port for the microWIU to function. Removal of this USB device disables the microWIU.</td></tr>
<tr><td>4</td><td>The microWIU checks for identical software versions between the unit and the programmed USB device. Since this is an initial installation, discrepancies are identified.

Software Integrity Check
<table><tr><th>Component</th><th>CPU-A</th><th>CPU-B</th></tr><tr><td>Non-Vital Software</td><td>OK</td><td></td></tr><tr><td>Vital Software</td><td>OK</td><td>OK</td></tr><tr><td>Vital Application</td><td>Update</td><td>Update</td></tr><tr><td>Vital FPGA</td><td>OK</td><td>OK</td></tr><tr><td>Vital VIDS</td><td>OK</td><td>OK</td></tr></table>
77%
Status: Status: Waiting for user input...
Application files have changed. Press next to verify CRC.

Select <b><i>Next</i></b>.</td></tr>
</table>

Table 3-2. Local Software Installation Procedure (Cont.)

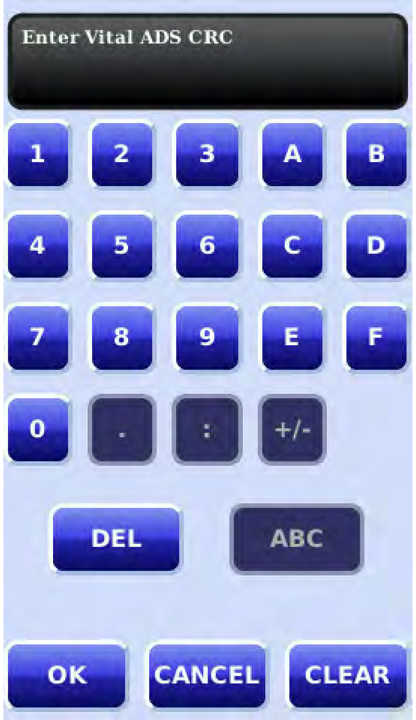
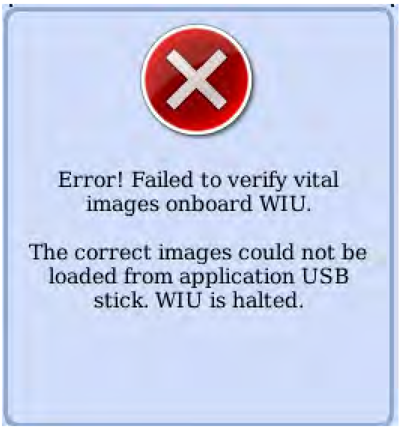
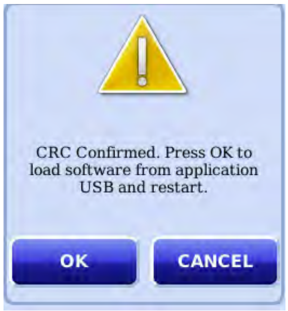
Step	Procedure
5	 Enter Vital ADS CRC 1 2 3 A B 4 5 6 C D 7 8 9 E F 0 . : +/- DEL ABC OK CANCEL CLEAR Enter the applicable CRC(s). Select ***OK***. Note: Using the remote web viewer (Section 3.3.2) is the easiest way to enter the CRCs.
6	 Error! Failed to verify vital images onboard WIU. The correct images could not be loaded from application USB stick. WIU is halted. If CRCs do not match, execution of the application is halted. User must investigate the cause of discrepancy (by re-entering the CRCs or re-validating the application) and correct before continuing.

Table 3-2. Local Software Installation Procedure (Cont.)

Step	Procedure
6a	 CRC Confirmed. Press OK to load software from application USB and restart. When CRCs are confirmed identical, select ***OK*** to load application software.
7	Record results on Table B-1, Line 3.
8	When installation is finished, the microWIU restarts and the Status screen appears on the microWIU display.
9	Record results on Table B-1, Line 4.
10	Verify the network configuration is correct per site-specific Book of Plans.
11	Record results on Table B-1, Line 5.
12	Perform field testing of the Application before placing the location into revenue service, by following the testing plan and safety plan testing requirements for the Application.
13	Record results on Table B-1, Line 6.

3.3.2 Remote Software Installation

WARNING

Prior to software installation, validation testing must confirm all application logic is correct.

Table 3-3. Remote Software Installation Procedure

Step	Procedure
1	From a PC containing the ADT program, launch a web browser. Note: Java™ SE Runtime Environment, minimum version 7, must be installed on the PC. This software is freely available from Oracle at http://www.oracle.com/technetwork/java/javase/downloads/index.html.
2	Enter the following in the address bar: https://192.168.10.1/.

Table 3-3. Remote Software Installation Procedure (Cont.)

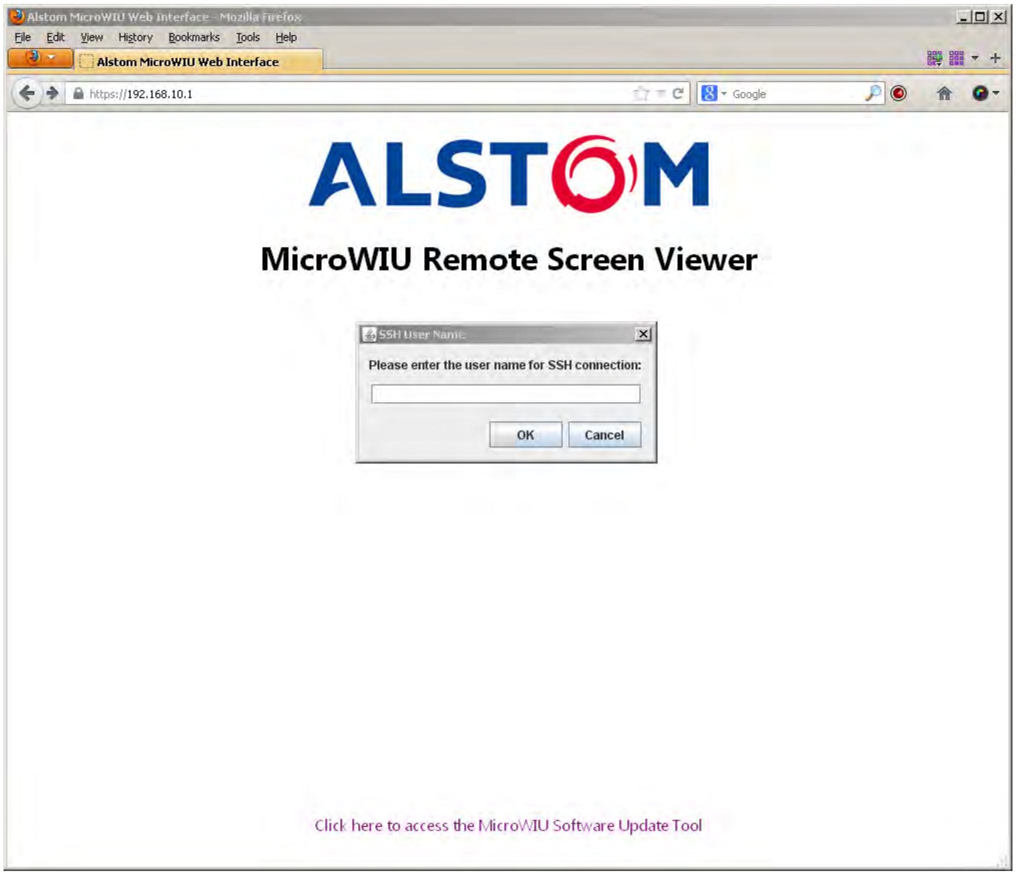
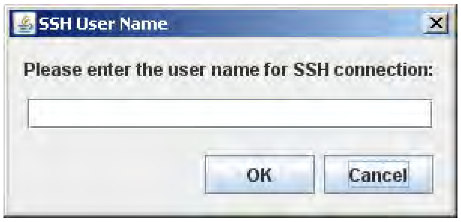
Step	**Procedure**
3	*The Alstom MicroWIU Remote Screen Viewer window opens.*  File Edit View History Bookmarks Tools Help Google ALSTOM OK Cancel Alstom MicroWIU Web Interface - Mozilla Firefox Alstom MicroWIU Web Interface https://192.168.10.1 MicroWIU Remote Screen Viewer SSH User Name Please enter the user name for SSH connection: Click here to access the MicroWIU Software Update Tool
3a	*The SSH User Name window also opens.*  SSH User Name Please enter the user name for SSH connection: Enter **microwiu**. Note: Username is case sensitive. Select ***OK***.

Table 3-3. Remote Software Installation Procedure (Cont.)

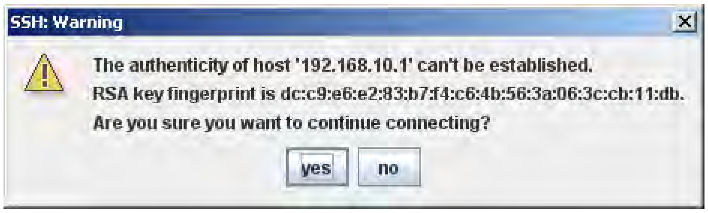
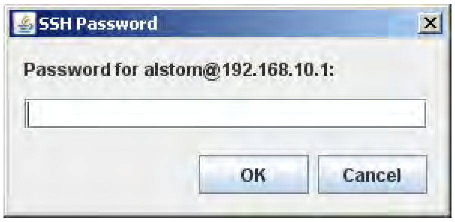
Step	Procedure
4	*The SSH Warning window opens.*  The authenticity of host '192.168.10.1' can't be established. RSA key fingerprint is dc:c9:e6:e2:83:b7:f4:c6:4b:56:3a:06:3c:cb:11:db. Are you sure you want to continue connecting? Select ***YES***.
5	*The SSH Password window opens.*  Password for alstom@192.168.10.1: Enter the microWIU System Password as set in the ADT ***Application Settings | Security*** tab.

Table 3-3. Remote Software Installation Procedure (Cont.)

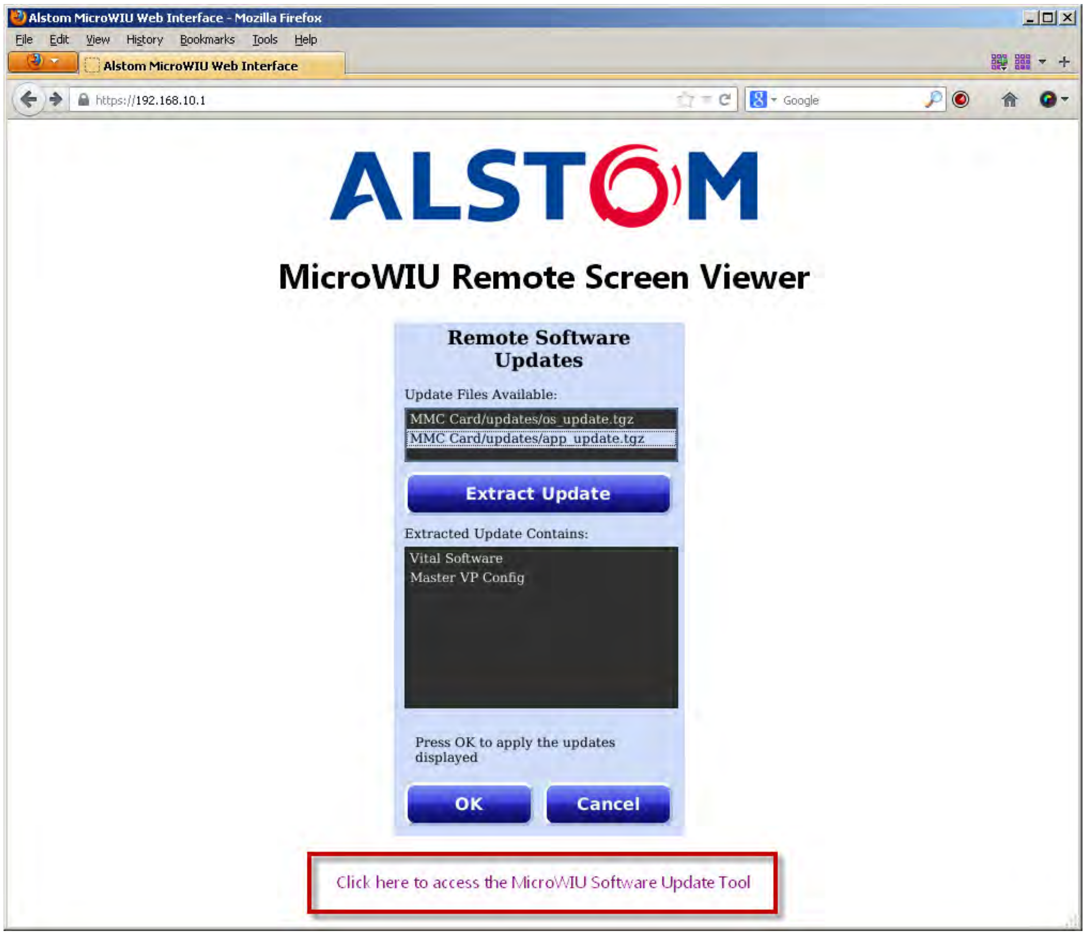
Step	Procedure
6	 Alstom MicroWIU Web Interface - Mozilla Firefox File Edit View History Bookmarks Tools Help Alstom MicroWIU Web Interface https://192.168.10.1 Google ALSTOM MicroWIU Remote Screen Viewer Remote Software Updates Update Files Available: MMC Card/updates/os_update.tgz MMC Card/updates/app_update.tgz Extracted Update Contains: Vital Software Master VP Config Press OK to apply the updates displayed Click here to access the MicroWIU Software Update Tool Click the line that states ***Click here to access the MicroWIU Software Update Tool.***

Table 3-3. Remote Software Installation Procedure (Cont.)

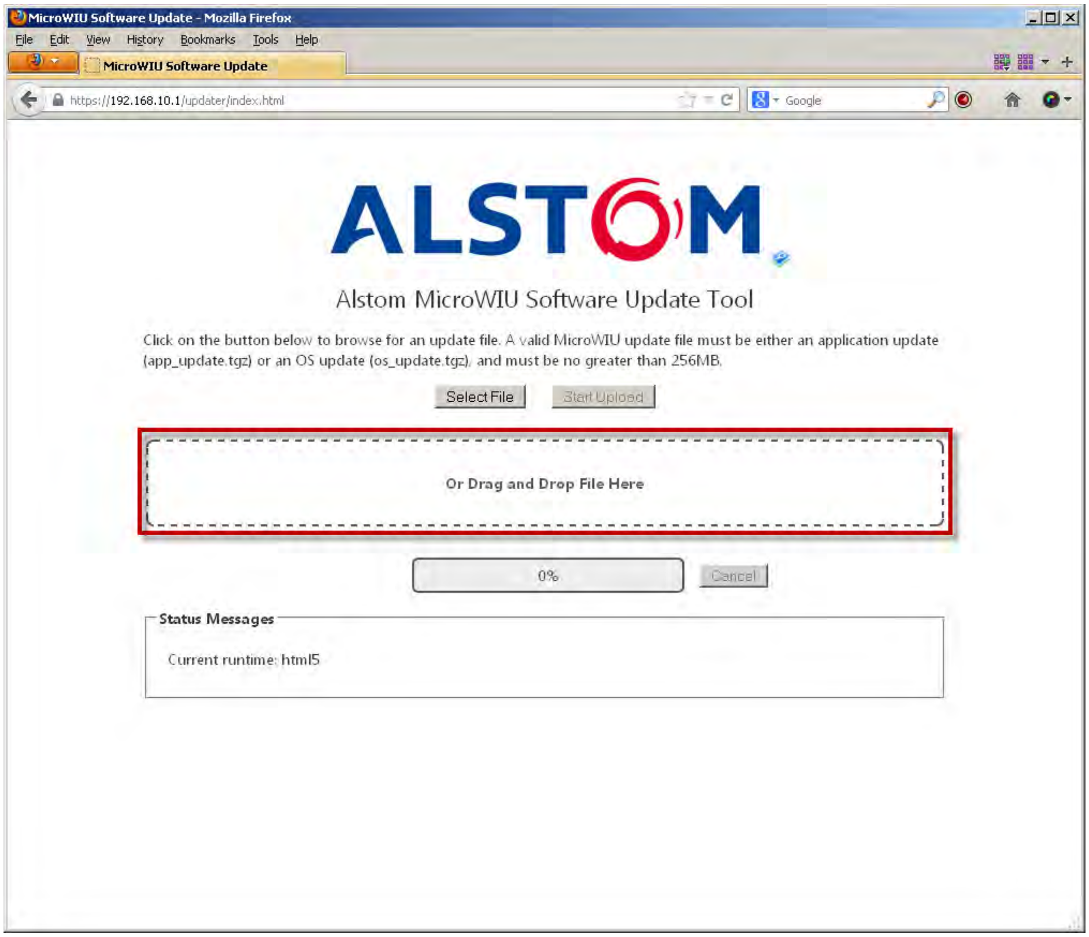
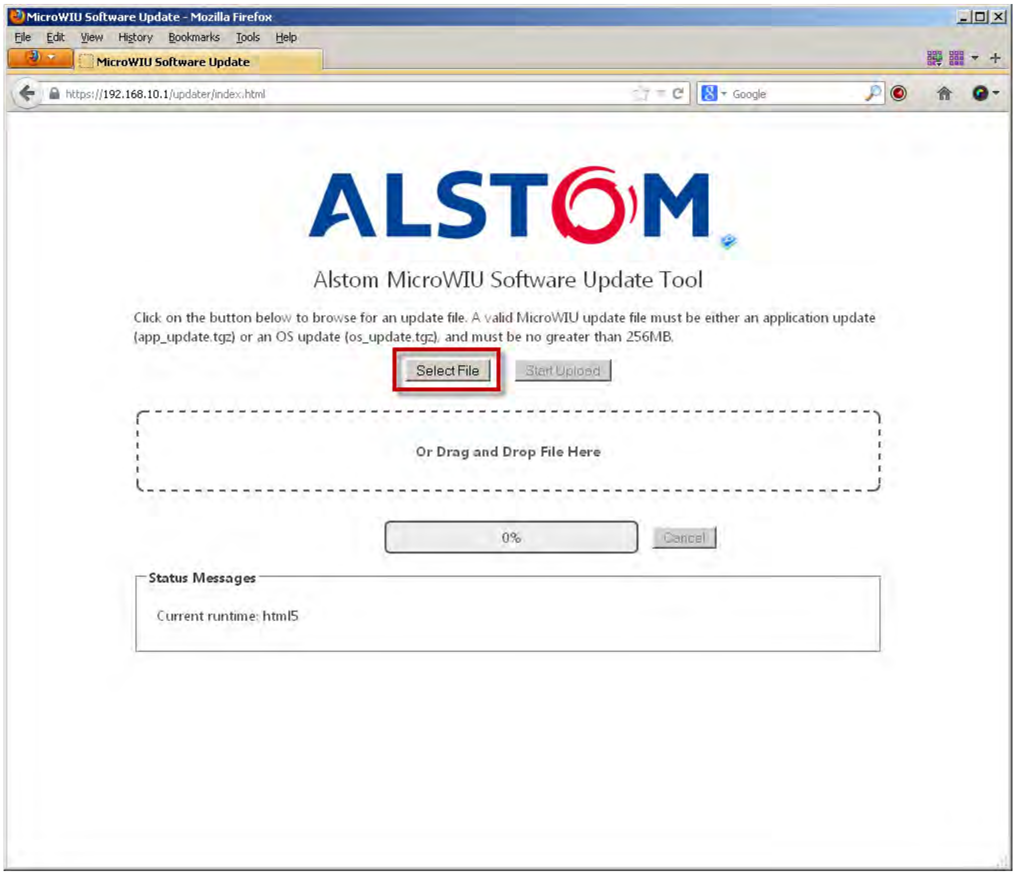
Step	Procedure
7	 MicroWIU Software Update - Mozilla Firefox File Edit View History Bookmarks Tools Help MicroWIU Software Update https://192.168.10.1/updater/index.html Google ALSTOM Select File Start Upload 0% Cancel Alstom MicroWIU Software Update Tool Click on the button below to browse for an update file. A valid MicroWIU update file must be either an application update (app_update.tgz) or an OS update (os_update.tgz), and must be no greater than 256MB. Or Drag and Drop File Here Status Messages Current runtime: html5 **Option 1:** Drag the (app_update.tgz) or an OS update (os_update.tgz) file into the Drag and Drop File Here area.

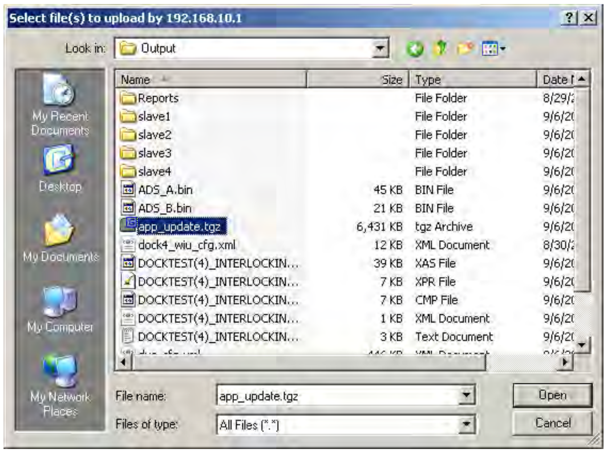
Table 3-3. Remote Software Installation Procedure (Cont.)

<table>
<tr><th>Step</th><th>Procedure</th></tr>
<tr><td>7a</td><td>

MicroWIU Software Update - Mozilla Firefox
File Edit View History Bookmarks Tools Help
MicroWIU Software Update
https://192.168.10.1/updater/index.html
Google
ALSTOM
Select File
Start Upload
Or Drag and Drop File Here
0%
Cancel
Status Messages

Alstom MicroWIU Software Update Tool

Click on the button below to browse for an update file. A valid MicroWIU update file must be either an application update (app_update.tgz) or an OS update (os_update.tgz), and must be no greater than 256MB.

Current runtime: html5



<table>
<tr><th>Name</th><th>Size</th><th>Type</th><th>Date I</th></tr>
<tr><td>Reports</td><td></td><td>File Folder</td><td>8/29/</td></tr>
<tr><td>slave1</td><td></td><td>File Folder</td><td>9/6/2(</td></tr>
<tr><td>slave2</td><td></td><td>File Folder</td><td>9/6/2(</td></tr>
<tr><td>slave3</td><td></td><td>File Folder</td><td>9/6/2(</td></tr>
<tr><td>slave4</td><td></td><td>File Folder</td><td>9/6/2(</td></tr>
<tr><td>ADS_A.bin</td><td>45 KB</td><td>BIN File</td><td>9/6/2(</td></tr>
<tr><td>ADS_B.bin</td><td>21 KB</td><td>BIN File</td><td>9/6/2(</td></tr>
<tr><td>app_update.tgz</td><td>6,431 KB</td><td>tgz Archive</td><td>9/6/2(</td></tr>
<tr><td>dock4_wiu_cfg.xml</td><td>12 KB</td><td>XML Document</td><td>8/30/</td></tr>
<tr><td>DOCKTEST(4)_INTERLOCKIN...</td><td>39 KB</td><td>XAS File</td><td>9/6/2(</td></tr>
<tr><td>DOCKTEST(4)_INTERLOCKIN...</td><td>7 KB</td><td>XPR File</td><td>9/6/2(</td></tr>
<tr><td>DOCKTEST(4)_INTERLOCKIN...</td><td>7 KB</td><td>CMP File</td><td>9/6/2(</td></tr>
<tr><td>DOCKTEST(4)_INTERLOCKIN...</td><td>1 KB</td><td>XML Document</td><td>9/6/2(</td></tr>
<tr><td>DOCKTEST(4)_INTERLOCKIN...</td><td>3 KB</td><td>Text Document</td><td>9/6/2(</td></tr>
</table>
File name: app_update.tgz

Files of type: All Files (*.*)

<b>Option 2:</b> Select <b><i>Select File</i></b>.

Browse to the Application update (app_update.tgz) or OS update (os_update.tgz) file to upload.

Select <b><i>Open</i></b>.
</td></tr>
</table>

Table 3-3. Remote Software Installation Procedure (Cont.)

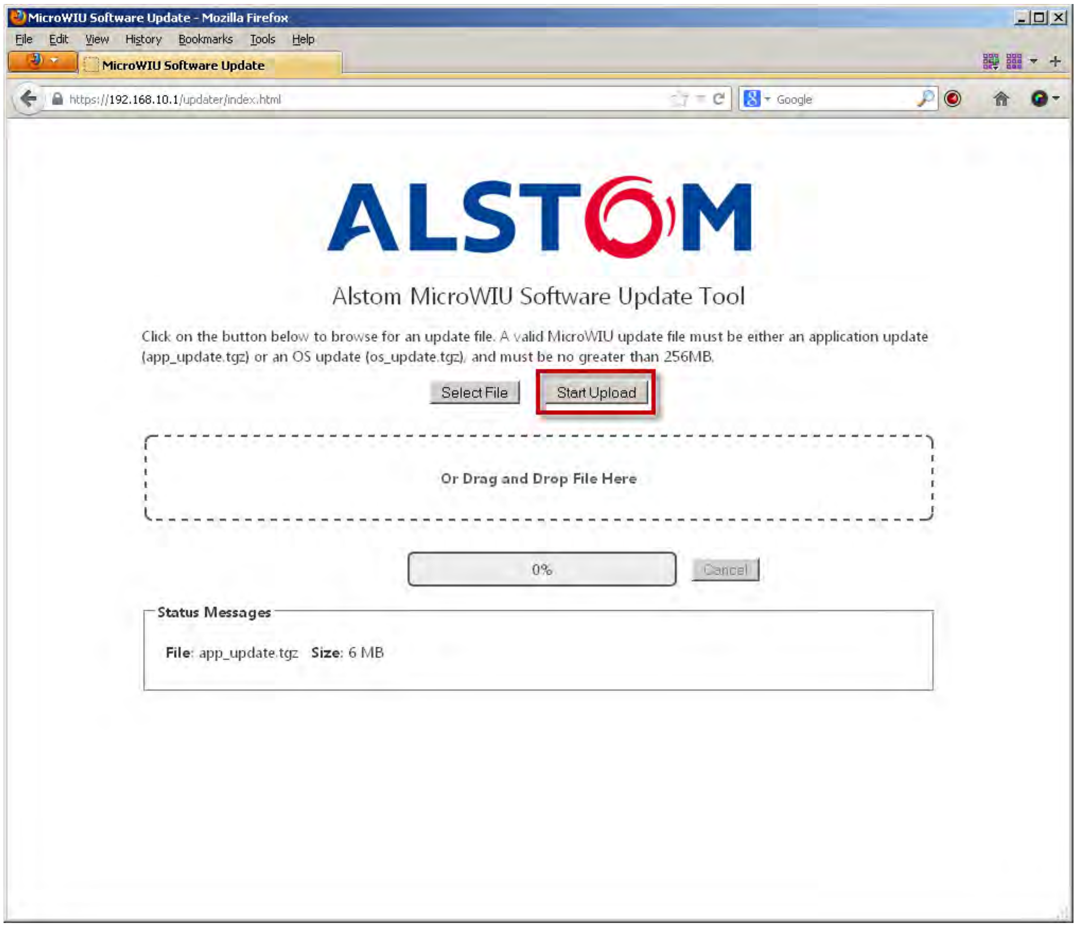
Step	Procedure
8	 MicroWIU Software Update - Mozilla Firefox File Edit View History Bookmarks Tools Help MicroWIU Software Update https://192.168.10.1/updater/index.html Google ALSTOM Select File Start Upload Or Drag and Drop File Here 0% CancelAlstom MicroWIU Software Update Tool Click on the button below to browse for an update file. A valid MicroWIU update file must be either an application update (app_update.tgz) or an OS update (os_update.tgz), and must be no greater than 256MB. Status Messages File: app_update.tgz Size: 6 MB Select ***Start Upload***.

Table 3-3. Remote Software Installation Procedure (Cont.)

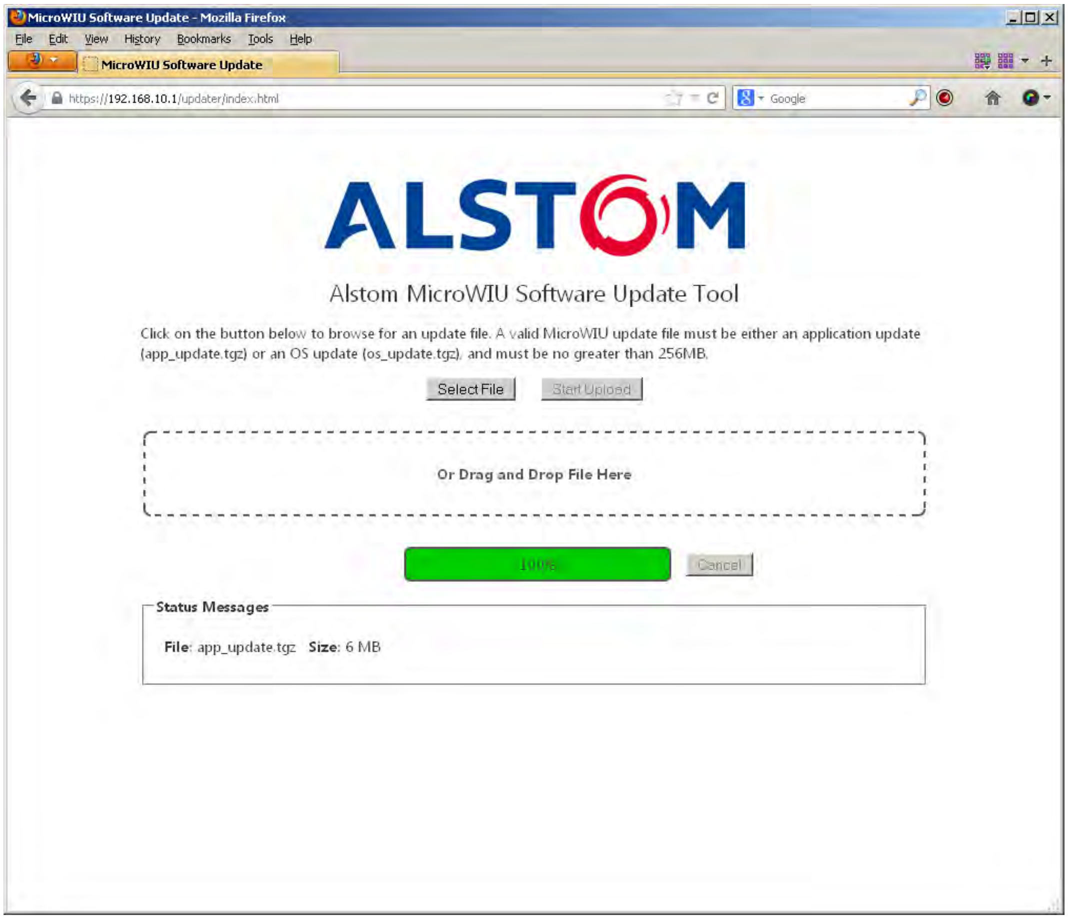
Step	Procedure
9	 MicroWIU Software Update - Mozilla Firefox File Edit View History Bookmarks Tools Help MicroWIU Software Update https://192.168.10.1/updater/index.html Google ALSTOM Select File Start Upload Or Drag and Drop File Here 100% Cancel Status Messages Alstom MicroWIU Software Update Tool Click on the button below to browse for an update file. A valid MicroWIU update file must be either an application update (app_update.tgz) or an OS update (os_update.tgz), and must be no greater than 256MB. **File**: app_update.tgz **Size**: 6 MB Once upload is complete, press the ***Confirm*** button on the Master or Standalone microWIU for one second.
10	Repeat Steps 2-5 to establish a connection again with the microWIU.

Table 3-3. Remote Software Installation Procedure (Cont.)

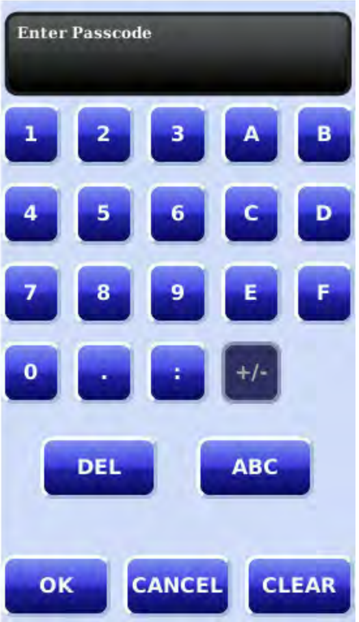
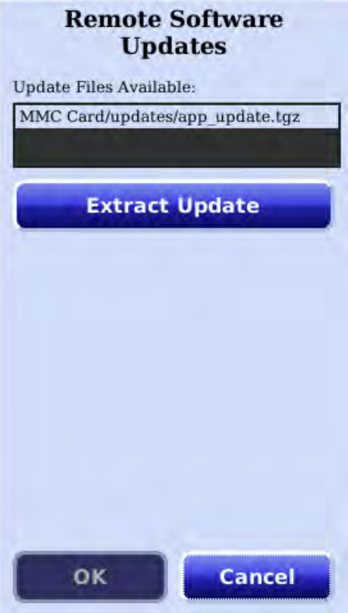
Step	Procedure
11	*MicroWIU screen is displayed, requiring a passcode to continue.*  Enter Passcode 1 2 3 A B 4 5 6 C D 7 8 9 E F 0 . : +/- DEL ABC OK CANCEL CLEAR Enter the security level passcode (PIN) as established in the ADT application. Select ***OK***.
12	*A new window opens.*  Remote Software Updates Update Files Available: MMC Card/updates/app_update.tgz Select ***Extract Update***.

Table 3-3. Remote Software Installation Procedure (Cont.)

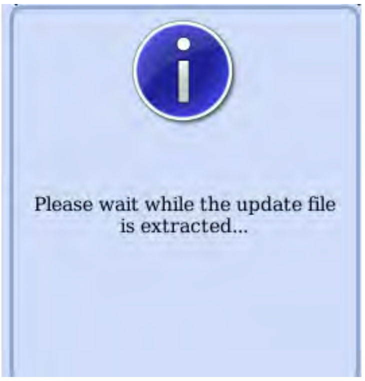
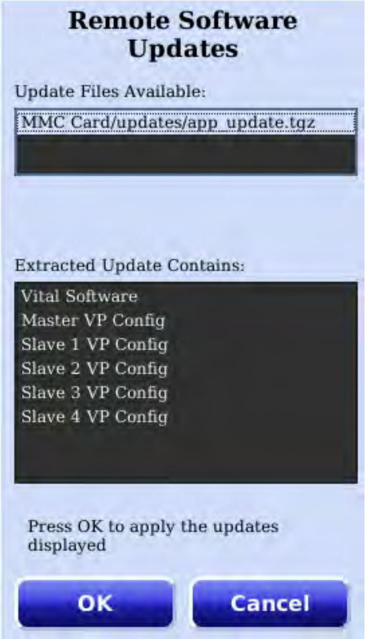
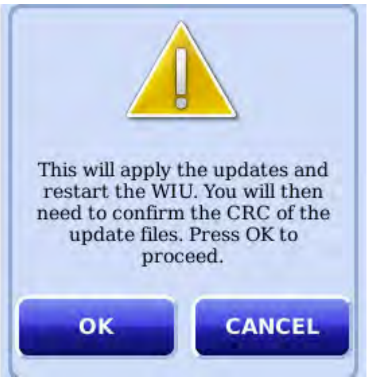
Step	Procedure
13	*The following windows open.*  Please wait while the update file is extracted...  **Remote Software Updates** Update Files Available: MMC Card/updates/app_update.tgz Extracted Update Contains: Vital Software Master VP Config Slave 1 VP Config Slave 2 VP Config Slave 3 VP Config Slave 4 VP Config Press OK to apply the updates displayed  This will apply the updates and restart the WIU. You will then need to confirm the CRC of the update files. Press OK to proceed. Select ***OK*** to apply the updates.

Table 3-3. Remote Software Installation Procedure (Cont.)

Step	Procedure
14	When CRCs are confirmed identical, select ***OK*** to load application software.
15	Record results on Table B-1, Line 3.
16	When installation is finished, the microWIU restarts and the Status screen appears on the microWIU display.
17	Record results on Table B-1, Line 4.
18	Verify the network configuration is correct per site-specific Book of Plans.
19	Record results on Table B-1, Line 5.
20	Perform field testing of the Application before placing the location into revenue service, by following the testing plan and safety plan testing requirements for the Application.
21	Record results on Table B-1, Line 6.

3.4 WIRING RECOMMENDATIONS

Note: For input wiring, use a wire gauge between 28 AWG and 12 AWG.

Note: For power wiring (12 VDC nominal), use a wire gauge between 16 AWG and 12 AWG.

Note: Keep Ethernet cables isolated from all other wiring (for example, high current, relay contact, or coil signal).

See Table 3–4 for signal-to-connector wiring connections.

Table 3–4. microWIU Wiring Connections

Signal	Connector	
Input 1+	J3-1	J3
Input 1–	J3-2	
Input 2+	J3-3	
Input 2–	J3-4	
Input 3+	J3-5	
Input 3–	J3-6	
Input 4+	J3-7	
Input 4–	J3-8	
Input 5+	J5-1	J5
Input 5–	J5-2	
Input 6+	J5-3	
Input 6–	J5-4	
Input 7+	J5-5	
Input 7–	J5-6	
Input 8+	J5-7	
Input 8–	J5-8	
Input 9+	J4-1	J4
Input 9–	J4-2	
Input 10+	J4-3	
Input 10–	J4-4	
Input 11+	J4-5	
Input 11–	J4-6	
Input 12+	J4-7	
Input 12–	J4-8	

Table 3–4. microWIU Wiring Connections (Cont.)

Signal	Connector	
Input 13+	J6-1	J6
Input 13–	J6-2	
Input 14+	J6-3	
Input 14–	J6-4	
Input 15+	J6-5	
Input 15–	J6-6	
Input 16+	J6-7	
Input 16–	J6-8	
OUT1	J1-1	J1
OUT2	J1-2	
12 COM	J1-3	
12 VDC	J1-4	
CANL CANH	J2-1 J2-2 shielded twisted pair	J2
CANL CANH	J2-3 J2-4 shielded twisted pair	

3.5 MASTER/SLAVE CONNECTIONS

The ability to stack the microWIU allows multiple units to be interconnected and appear to a PTC network as a single, large WIU. This increases the input count up to 112 Vital inputs (43 inputs with Extended CAN Bus) and 14 non-vital outputs with 7 stacked units.

For Master/Slave wiring, use a wire gauge between 28 AWG and 12 AWG. Keep wire lengths between units as short as possible (up to 100 ft for normal applications and up to 1500 ft for Extended CAN bus). Wire lengths should be twisted (1 twist per ft minimum). Resistors (120 Ω, 0.25 W) must be installed at the first and last units in the chain. See Figure 3-2 for wiring details.

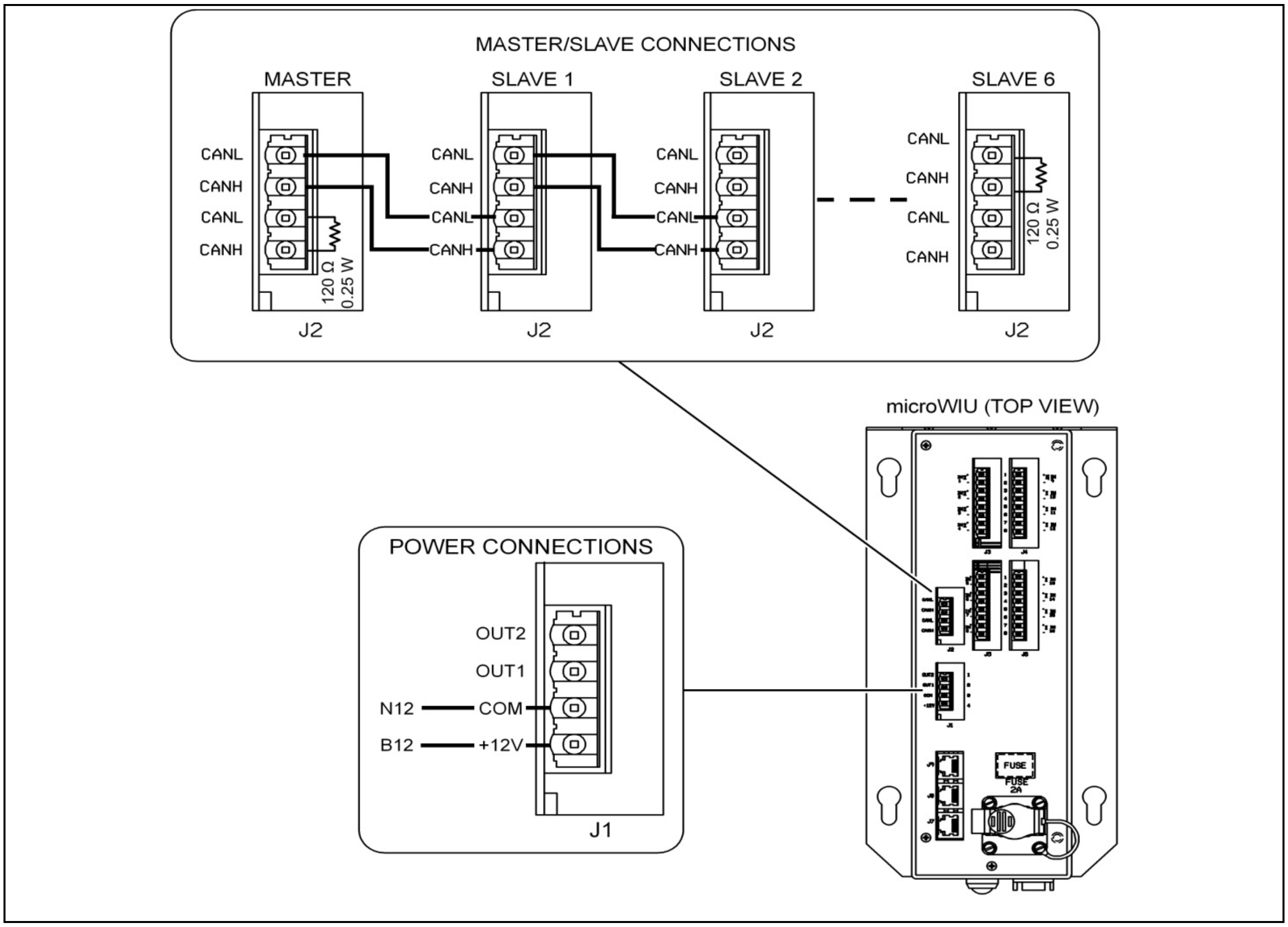


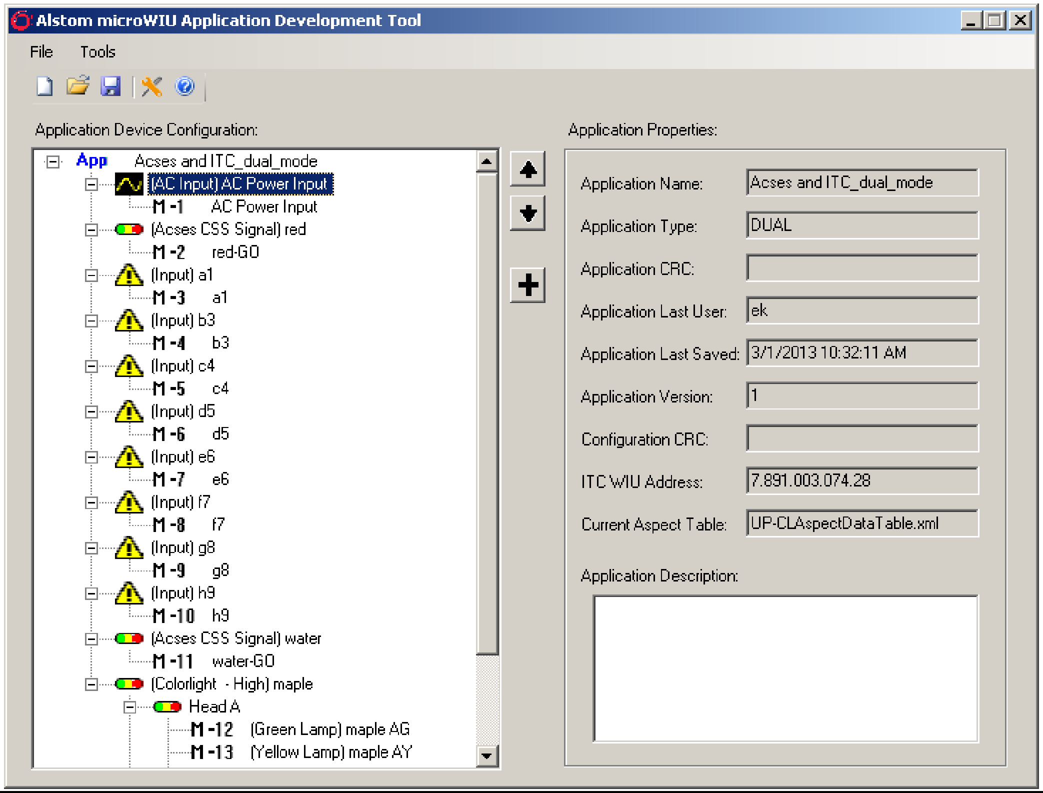
Figure 3-2. Master/Slave Connections

Note: When using VSOE2 on a microWIU system, the concept of master/slave is no longer applicable. VSOE2 resides only on what was the master, and carries 16 local inputs. All of the remaining inputs sent in from a VSOE2 message are accepted and processed by the master unit. Should a master still be connected to a slave, the slave is ignored.

3.6 AC POWER DETECTION

If the site-configured application loaded onto the microWIU has an AC Power Input, the input port must be configured.

In Figure 3-3, an AC Power Input was added as Input 1 on the master unit.


Alstom microWIU Application Development Tool
File
Tools
Application Device Configuration:
Application Properties:

```
App    Acses and ITC_dual_mode
  (AC Input) AC Power Input
    M -1    AC Power Input
  (Acses CSS Signal) red
    M -2    red-GO
  (Input) a1
    M -3    a1
  (Input) b3
    M -4    b3
  (Input) c4
    M -5    c4
  (Input) d5
    M -6    d5
  (Input) e6
    M -7    e6
  (Input) f7
    M -8    f7
  (Input) g8
    M -9    g8
  (Input) h9
    M -10   h9
  (Acses CSS Signal) water
    M -11   water-GO
  (Colorlight - High) maple
    Head A
      M -12   (Green Lamp) maple AG
      M -13   (Yellow Lamp) maple AY
```

Application Name:	Acses and ITC_dual_mode
Application Type:	DUAL
Application CRC:	
Application Last User:	ek
Application Last Saved:	3/1/2013 10:32:11 AM
Application Version:	1
Configuration CRC:	
ITC WIU Address:	7.891.003.074.28
Current Aspect Table:	UP-CLAspectDataTable.xml
Application Description:	

Figure 3-3. AC Power Input Example

An AC relay coil needs to be wired to the AC power input as per the loaded application. Wire a relay contact to the +12V input and another contact to the microWIU input as defined in ADT (input 1 in this example). Refer to the drawing below for an example of relay wiring.

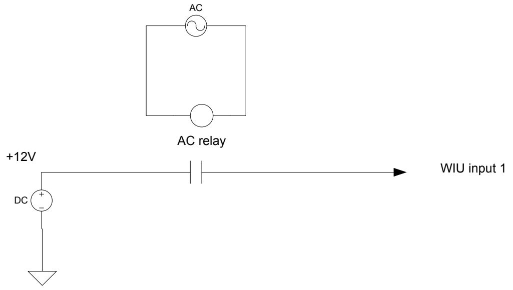


Figure 3-4. Example AC Power Wiring Diagram

SECTION 4 – OPERATION

4.1 GENERAL

This section provides instructions for the operation of the Alstom microWIU.

WARNING

Field testing of an Application is required before placing the location into revenue service. The customer's testing plan and safety plan define the testing requirements for the Application.

WARNING

Railroad correspondence (validation) testing must be conducted to ensure that microWIU configuration and physical connections agree with railroad track conditions.

WARNING

Railroad personnel, using the verification and validation process, must ensure that the microWIU is programmed with the correct application logic and consistent with application requirements.

WARNING

Railroad personnel, using the verification and validation process, must ensure that the microWIU is correctly configured.

WARNING

Personnel must be trained and qualified, in accordance with the product installation or maintenance manuals, before installing or servicing microWIU equipment.

WARNING

It is the railroad's responsibility to establish and maintain the Security Levels through the ADT for microWIU window access. Restriction of unauthorized personnel to functions that can affect safety is imperative.

WARNING

It is the railroad's responsibility to ensure remote access via a TCP/IP connection is secured and controlled by a passcode.

CAUTION

Proper PTC operation must be verified by field test before use and after any repair.

CAUTION

Product manuals clearly define all maintenance requirements of the system, and training must be sufficient to convey understanding of safety requirements.

CAUTION

Use of the Application Development Tool must be limited to only skilled and trained application designers (application engineers).

4.2 USER INTERACTION

When WIU units are installed and commissioned as part of a PTC system, they operate autonomously without direct user interaction.

User interaction is required for:

- Initial Configuration: Each WIU product requires configuration for its operating location, functional operating parameters, communication link settings, etc.; this is performed by an Application Engineer from Alstom, the railroad, or the contractor
- Maintenance and Field Configuration: Troubleshooting and replacements are performed by the railroad or contractor as required; field configuration is performed by the railroad maintenance staff, and includes software updates and encryption key updates
- Operational Configuration and Status (Ethernet web server interface and touch screen display): The User Interfaces for configuration and status of the microWIU consist of:
  - An embedded Ethernet web server interface as a primary operational user interface for configuration and status
  - A touch screen display as a secondary operational user interface for configuration and status

4.3 USER INTERFACE ACCESS

All maintenance functions, such as viewing Train Response Messages, communications status, real-time input states, are available through both the microWIU Touch-Screen Display interface and through the embedded Web-Server interface.

To access the web-server, connect a standard Ethernet cable between the microWIU and a laptop/PC. Launch a web browser window (either Internet Explorer or Firefox) and navigate to the pre-configured web page address of the microWIU.

The built-in touch screen displays the interaction from the web server interface in real time. The touch screens update as they are selected or altered via the web server.

Table 4–1. Accessing the Embedded Web Server Interface

Step	**Action**
1	Plug an Ethernet cable into an available Ethernet port on the microWIU and connect to a laptop or PC.
2	Open a web browser. If using Internet Explorer, proceed to Step 2a to trust the website security certificate. If using Firefox, proceed to Step 3 to trust the website security certificate.
2a	For the first time using remote login using the Internet Explorer web browser, select ***Tools* | *Internet Options* | *Advanced.***

Table 4–1. Accessing the Embedded Web Server Interface (Cont.)

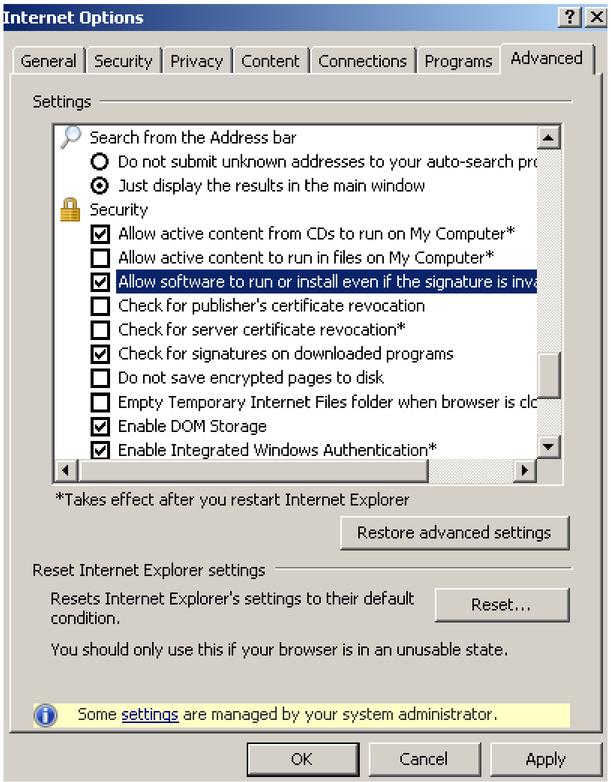
Step	Action
2b	*The Internet Options window opens.*  Internet Options General · Security · Privacy · Content · Connections · Programs · Advanced Settings Search from the Address bar ○ Do not submit unknown addresses to your auto-search pr ● Just display the results in the main window Security ☑ Allow active content from CDs to run on My Computer* ☐ Allow active content to run in files on My Computer* ☑ Allow software to run or install even if the signature is inva ☐ Check for publisher's certificate revocation ☐ Check for server certificate revocation* ☑ Check for signatures on downloaded programs ☐ Do not save encrypted pages to disk ☐ Empty Temporary Internet Files folder when browser is cl ☑ Enable DOM Storage ☑ Enable Integrated Windows Authentication* *Takes effect after you restart Internet Explorer Restore advanced settings Reset Internet Explorer settings Resets Internet Explorer's settings to their default condition. Reset... You should only use this if your browser is in an unusable state. Some settings are managed by your system administrator. OK · Cancel · Apply Scroll down to 'Security' and verify option ‘Allow software to run or install even if the signature is invalid’ is checked. Select ***Apply***. Select ***OK***.

Table 4–1. Accessing the Embedded Web Server Interface (Cont.)

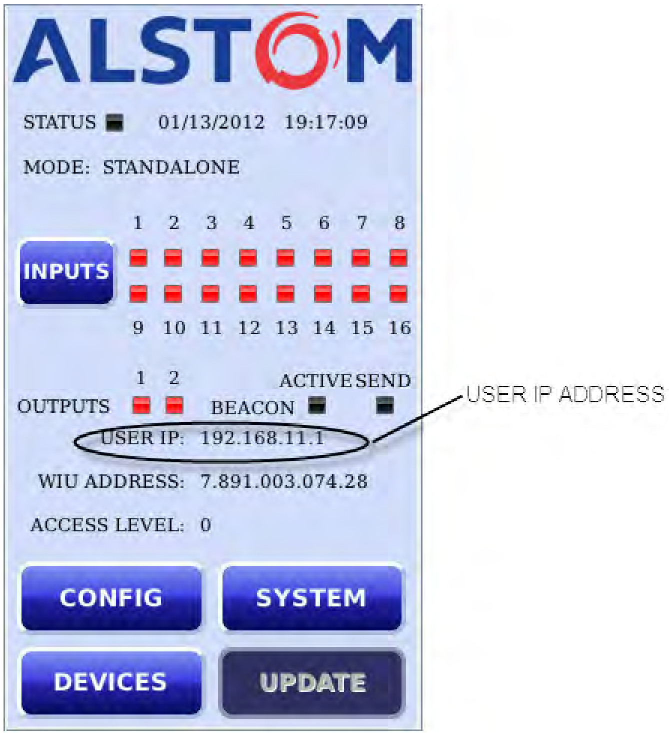
Step	Action
3	In the web browser’s address field, enter the User IP address for the embedded web server interface as shown on the status screen of the microWIU’s built-in touch screen. As microWIU requires a secure web connection, be certain to use https:// when entering the IP address. For example, in the figure below the entered information would be https://192.168.11.1  STATUS ■ 01/13/2012 19:17:09 MODE: STANDALONE USER IP: 192.168.11.1 WIU ADDRESS: 7.891.003.074.28 ACCESS LEVEL: 0 ALSTOM INPUTS 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 OUTPUTS 1 2 ACTIVE SEND BEACON USER IP ADDRESS CONFIG SYSTEM DEVICES UPDATE

Table 4–1. Accessing the Embedded Web Server Interface (Cont.)

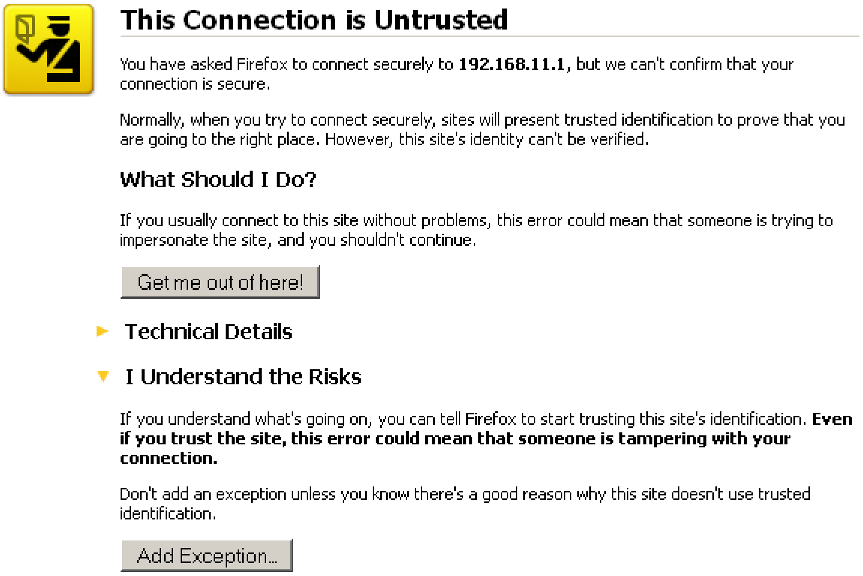
Step	Action
3a	For the first time using remote login using the Firefox web browser, a warning window opens as shown below.  **This Connection is Untrusted** You have asked Firefox to connect securely to **192.168.11.1**, but we can't confirm that your connection is secure. Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified. **What Should I Do?** If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue. ► Technical Details ▼ I Understand the Risks If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.** Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification. Select ***I Understand the Risks*** Select ***Add Exception…*** to trust this connection.

Table 4–1. Accessing the Embedded Web Server Interface (Cont.)

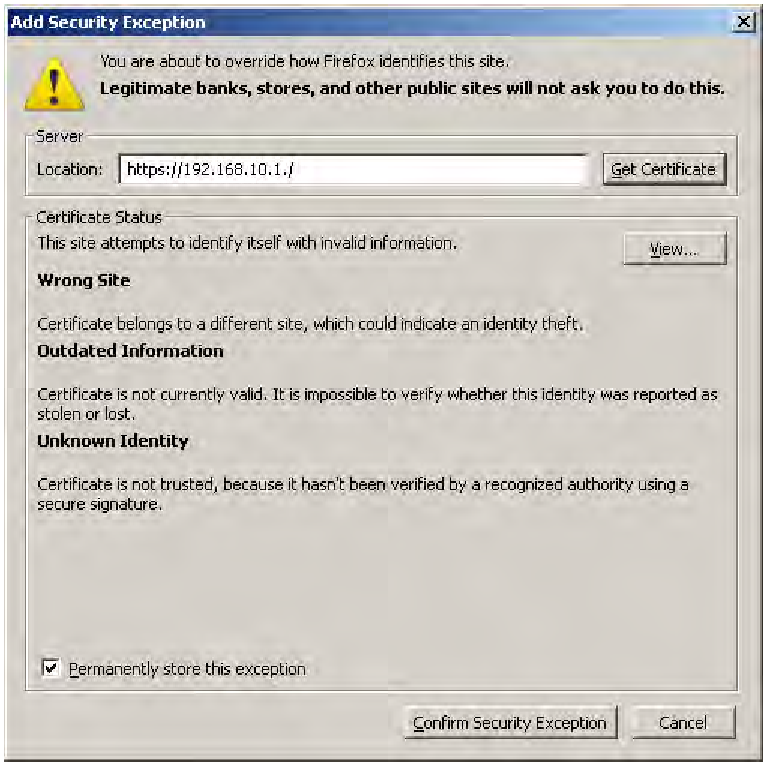
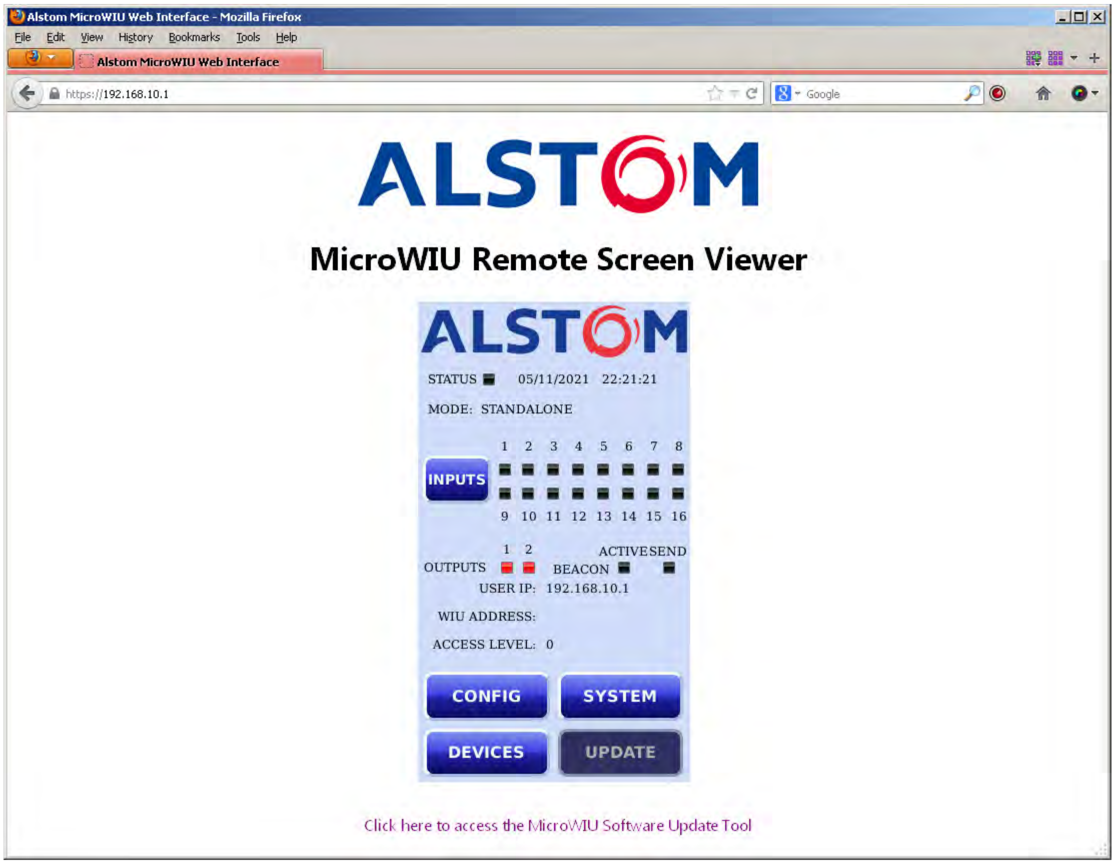
Step	Action
3b	 Add Security Exception Get Certificate View... Confirm Security Exception Cancel You are about to override how Firefox identifies this site. **Legitimate banks, stores, and other public sites will not ask you to do this.** Server Location: https://192.168.10.1./ Certificate Status This site attempts to identify itself with invalid information. **Wrong Site** Certificate belongs to a different site, which could indicate an identity theft. **Outdated Information** Certificate is not currently valid. It is impossible to verify whether this identity was reported as stolen or lost. **Unknown Identity** Certificate is not trusted, because it hasn't been verified by a recognized authority using a secure signature. ☑ Permanently store this exception Select the ***Permanently store the exception*** checkbox. Select ***Confirm Security Exception***.

Table 4–1. Accessing the Embedded Web Server Interface (Cont.)

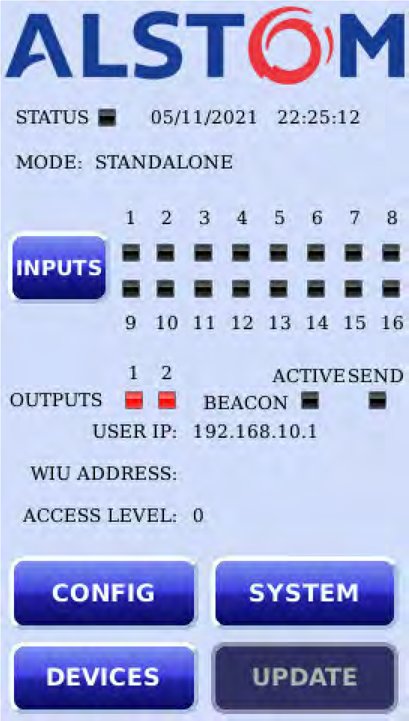
Step	Action
4	When the web server interface opens, the microWIU touch screen appears on the monitor. The monitor displays the touch screen, while the mouse and keyboard are used to interact with the web server interface.  Alstom MicroWIU Web Interface - Mozilla Firefox https://192.168.10.1 MicroWIU Remote Screen Viewer STATUS ■ 05/11/2021 22:21:21 MODE: STANDALONE USER IP: 192.168.10.1 WIU ADDRESS: ACCESS LEVEL: 0 Click here to access the MicroWIU Software Update Tool File Edit View History Bookmarks Tools Help Alstom MicroWIU Web Interface Google ALSTOM ALSTOM INPUTS 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 OUTPUTS 1 2 BEACON ACTIVESEND CONFIG SYSTEM DEVICES UPDATE

For more information on user interface operation applicable to both the unit and the web interface, see Section 4.4.

4.4 USER INTERFACE OPERATION

4.4.1 Status Screen

When the microWIU is powered on and the boot process is complete, the top level Status screen is displayed. All of the following microWIU touch screens are also viewed on the web interface when the unit is connected via Ethernet connection.



STATUS 05/11/2021 22:25:12

MODE: STANDALONE

USER IP: 192.168.10.1

WIU ADDRESS:

ACCESS LEVEL: 0

Figure 4-1. Example microWIU Top Level Status Screen

See Table 4–2 for descriptions of the Status screen indicators and buttons.

Table 4–2. Status Screen Indicators and Buttons

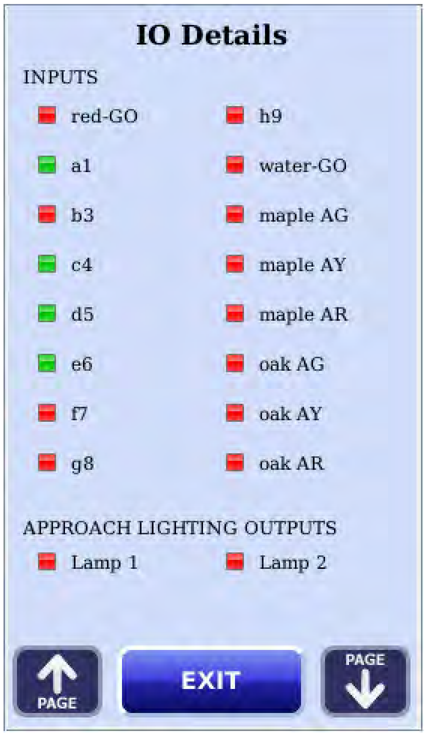
Indicator/Button	Description
Indicators	
STATUS	Displays Health Status Indication (Green/Yellow/Red).
MODE	Displays the function of the unit
INPUTS	Displays current states of Inputs 1–16 (Green = ON, Black = unused, Red = OFF)
OUTPUTS	Displays current states of Non-vital Outputs 1–2 (Green = ON, Red = OFF)
BEACON	Displays ITC Beacon status: • ACTIVE is ON (Green) when Beacon Time to Live (TTL) bit set in WSM • SEND blinks ON (Green) on WSM transmit
USER IP	Displays the embedded web server address
WIU ADDRESS	Displays the microWIU address (location configuration data)
ACCESS LEVEL	Displays the security level of the logged-in user (0 = read-only access, 1 and 2 = access granted to configuration parameters) The ADT defines which parameters are accessible at each access level, and whether a parameter can be changed at the microWIU or only from the ADT.
Buttons	
INPUTS	Select to open the IO Details screen.
CONFIG	Select to open the Configuration screen.
SYSTEM	Select to open the System screen.
DEVICES	Select to open the Devices screen.
UPDATE	Select to open the File Manager screen (enabled only when a USB device is inserted into the WIU. Note: The functions on the File Manager screen should only be performed by qualified personnel.

4.4.2 IO Details Screen

The IO Details screen correlates the real-time state of inputs with location signal names in order to aid in maintenance.

> Note: The IO Details screen does not require a passcode entry in order to view the screen.

Table 4–3. Accessing the IO Details Screen

Step	Action
1	From the Status screen, select the ***INPUTS*** button. *The IO Details screen opens.*  IO Details INPUTS 🟥 red-GO 🟥 h9 🟩 a1 🟥 water-GO 🟥 b3 🟥 maple AG 🟩 c4 🟥 maple AY 🟩 d5 🟥 maple AR 🟩 e6 🟥 oak AG 🟥 f7 🟥 oak AY 🟥 g8 🟥 oak AR APPROACH LIGHTING OUTPUTS 🟥 Lamp 1 🟥 Lamp 2 • **INPUTS:** Displays Vital input state information with the associated signal names assigned by the user during application development • **APPROACH LIGHTING OUTPUTS:** Displays non-vital output state information with the associated signal names assigned by the user during application development • **PAGE UP/DOWN:** Select the appropriate button to scroll up or down through the list of input and output display states
2	Select ***EXIT*** to return to the Status screen.

4.4.3 Configuration Screen

The Configuration screen provides access to configurable system parameters.

> Note: The ADT defines which parameters are accessible at each access level, and whether a parameter can be changed at the microWIU or only from the ADT.

Table 4–4. Accessing the Configuration Screen

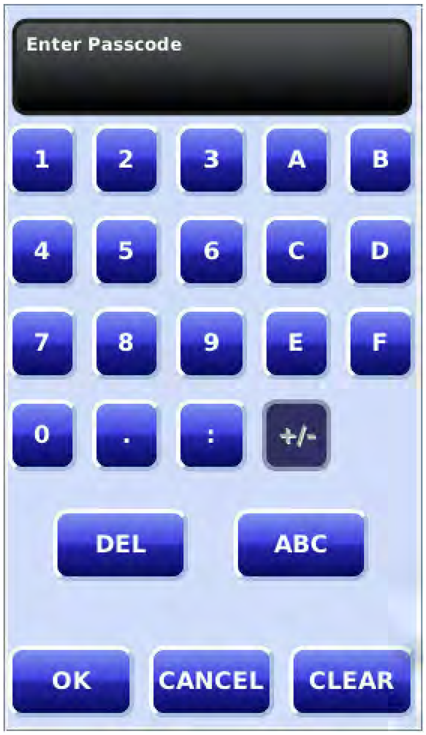
Step	Action
1	From the Status screen, select the ***CONFIG*** button.
2	*If not already logged in, the Enter Passcode screen opens.* Note: The Configuration screen requires the user to enter a valid passcode in order to access the configurable system parameters. This passcode is the same as the PIN assigned in the ADT, Application Settings | Security tab.  Enter Passcode 1 2 3 A B 4 5 6 C D 7 8 9 E F 0 . : +/- DEL ABC OK CANCEL CLEAR Enter a valid alphanumeric passcode and select ***OK***.

Table 4–4. Accessing the Configuration Screen (Cont.)

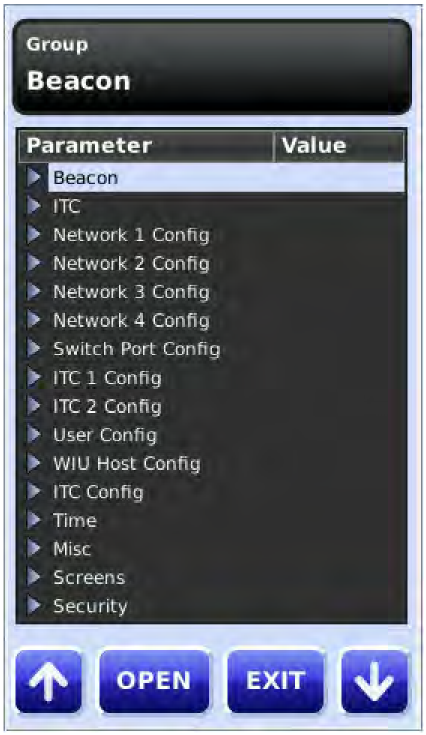
Step	Action
3	*The Configuration screen opens. The available configurable system parameters are displayed.*  Group Beacon Parameter Value Beacon ITC Network 1 Config Network 2 Config Network 3 Config Network 4 Config Switch Port Config ITC 1 Config ITC 2 Config User Config WIU Host Config ITC Config Time Misc Screens Security OPEN EXIT Select the arrow buttons to scroll to the intended function and select ***OPEN***. The selected function expands and shows the associated configurable items.

Table 4–4. Accessing the Configuration Screen (Cont.)

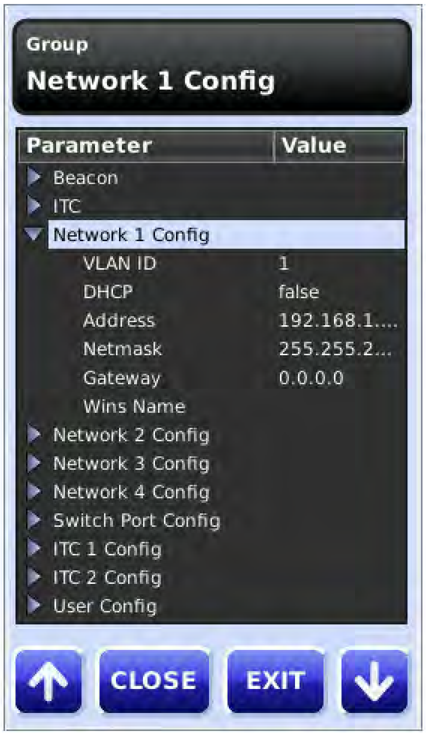
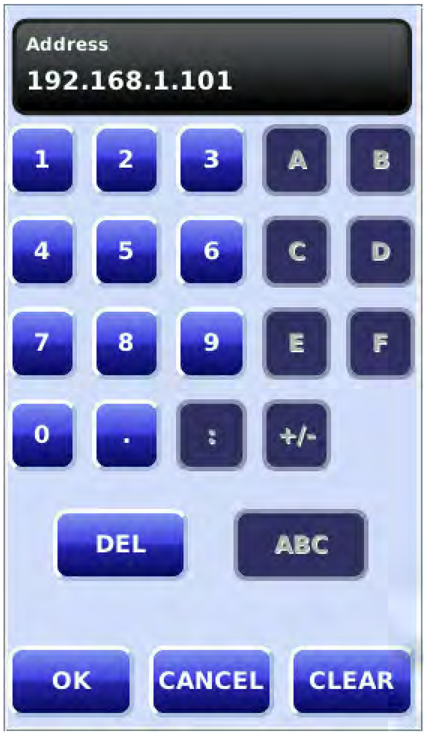
Step	Action
4	*In the example below, Network 1 Config was selected.*  Group Network 1 Config Parameter — Value ▶ Beacon ▶ ITC ▼ Network 1 Config VLAN ID — 1 DHCP — false Address — 192.168.1.... Netmask — 255.255.2... Gateway — 0.0.0.0 Wins Name ▶ Network 2 Config ▶ Network 3 Config ▶ Network 4 Config ▶ Switch Port Config ▶ ITC 1 Config ▶ ITC 2 Config ▶ User Config Use the arrow buttons to scroll to the intended configurable item. The ***CLOSE*** button changes to the ***EDIT*** button. Select ***EDIT*** to edit the configurable item.

Table 4–4. Accessing the Configuration Screen (Cont.)

Step	Action
5	*In the example below, Address was selected.*  Address 192.168.1.101 1 2 3 A B 4 5 6 C D 7 8 9 E F 0 . : +/- DEL ABC OK CANCEL CLEAR Use the web server screen (or built-in touch screen) to edit the selected item as needed. Select ***OK*** when done to save the changes. The previous screen reopens. Note: When an IP address is changed and a new Application is downloaded to the microWIU, the microWIU must be powered down and restarted in order for the new IP address change to be accepted.
6	Repeat Steps 4 and 5 to edit more configurable functions. When done, select ***EXIT*** to return to the Status screen.

4.4.4 System Screen

The System screen provides access to system level data and options, such as:

- Ethernet status/assigned IP address
- **VERSION**: configuration/version information is displayed for the following:
  - Config CRC configuration
  - NV application version and date
  - Serial Number and Board Revision
  - Library CRC
  - For each Vital CPU's A and B: Software version, Software CRC, FPGA version, FPGA CRC and App Data CRC
- **SET TIME**: set the system date and time
- **RESTART**: restart the microWIU
- **SHUTDOWN**: shut down the microWIU
- **LINKS**: provide connection status (ACSES, ITC, VSOE)
- **LOG**: view the event log
- **LOGOUT**: log out as user, setting Access Level back to 0
- **EXIT**: exit the window and return to Status screen

Table 4–5. Accessing the System Screen

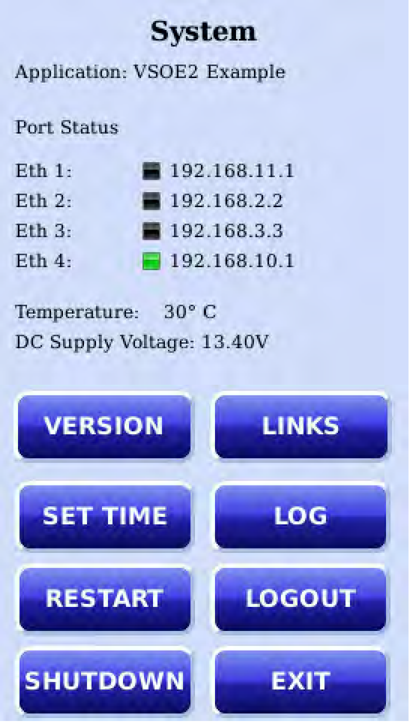
Step	Action
1	From the Status screen, select the ***SYSTEM*** button. Note: If not already logged in, the Enter Passcode screen opens. See Step 2 in Table 4–4 for passcode entry instructions.
2	*The System screen opens.*  System Application: VSOE2 Example Port Status Eth 1: ■ 192.168.11.1 Eth 2: ■ 192.168.2.2 Eth 3: ■ 192.168.3.3 Eth 4: 🟩 192.168.10.1 Temperature: 30° C DC Supply Voltage: 13.40V VERSION LINKS SET TIME LOG RESTART LOGOUT SHUTDOWN EXIT To: • View the version information, see Step 3 • Set the system date and time, see Step 5 • Restart the microWIU, see Step 8 • Shutdown the microWIU, see Step 10 • Links showing connection status, see Step 12 • Log monitors the event log, see Step 14 • Log out of the microWIU, see Step 16 • Exit the System window and return to the main screen, see Step 18
3	To view the version information, select the ***VERSION*** button.

Table 4–5. Accessing the System Screen (Cont.)

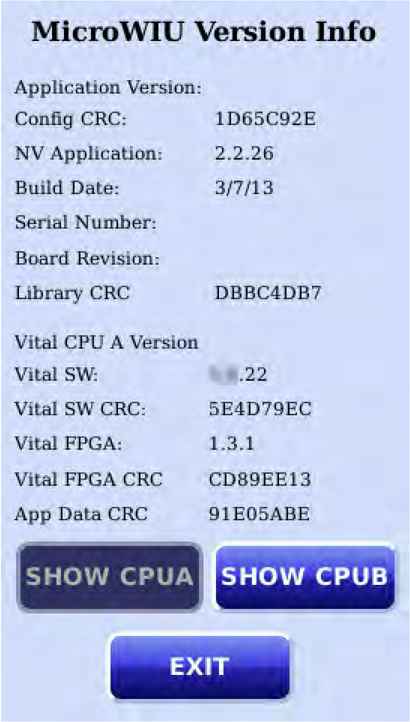
Step	Action
4	*The Version Display screen opens.*  **MicroWIU Version Info** Application Version: Config CRC: 1D65C92E NV Application: 2.2.26 Build Date: 3/7/13 Serial Number: Board Revision: Library CRC DBBC4DB7 Vital CPU A Version Vital SW: [redacted].22 Vital SW CRC: 5E4D79EC Vital FPGA: 1.3.1 Vital FPGA CRC CD89EE13 App Data CRC 91E05ABE Select ***EXIT*** to return to the System screen.
5	To set the system date and time, select the ***SET TIME*** button.

Table 4–5. Accessing the System Screen (Cont.)

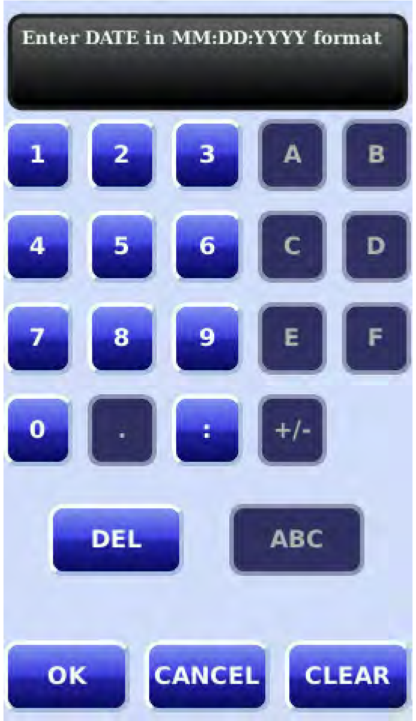
Step	Action
6	*The Set Date screen opens.*  Enter DATE in MM:DD:YYYY format 1 2 3 A B 4 5 6 C D 7 8 9 E F 0 . : +/- DEL ABC OK CANCEL CLEAR Enter the current date in MM:DD:YY format. Select ***OK*** when done. Note: Make sure to select the “**:**” (colon) button to separate the month/date/year entries.

Table 4–5. Accessing the System Screen (Cont.)

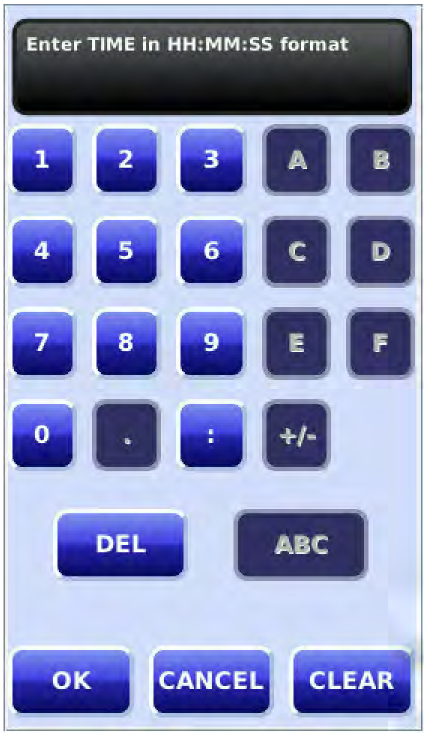
Step	Action
7	*The Set Time screen opens.*  Enter TIME in HH:MM:SS format 1 2 3 A B 4 5 6 C D 7 8 9 E F 0 . : +/- DEL ABC OK CANCEL CLEAR Enter the current time in HH:MM:SS format. Select ***OK*** when done. Note: Make sure to use “**:**” (colon) button to separate the hour/minutes/year entries.
8	To restart the microWIU, select the ***RESTART*** button.

Table 4–5. Accessing the System Screen (Cont.)

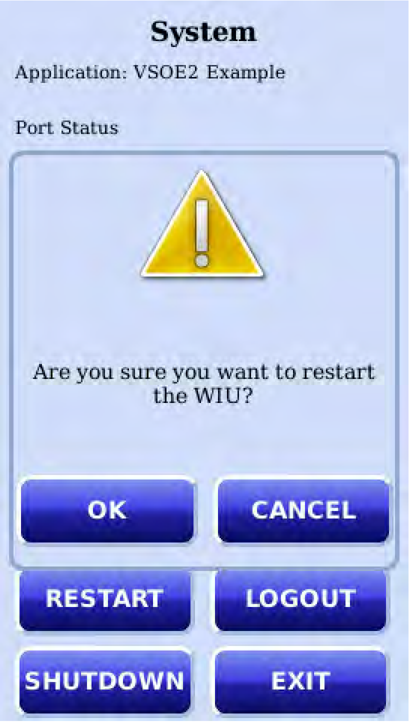
Step	Action
9	*A system prompt asks for confirmation of the restart.*  System Application: VSOE2 Example Port Status Are you sure you want to restart the WIU? Select ***OK*** to continue with the restart. The microWIU restarts and returns to the Status screen. The user who was logged in is now logged out.
10	To shut down the microWIU, select the ***SHUTDOWN*** button.

Table 4–5. Accessing the System Screen (Cont.)

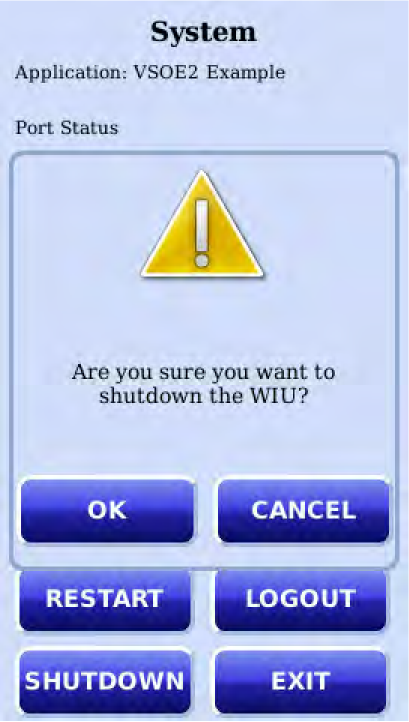
Step	Action
11	*A system prompt asks for confirmation of the shutdown.*  System Application: VSOE2 Example Port Status Are you sure you want to shutdown the WIU? Select ***OK*** to shut down the unit.
12	To display the connection status links, select the ***LINKS*** button.

Table 4–5. Accessing the System Screen (Cont.)

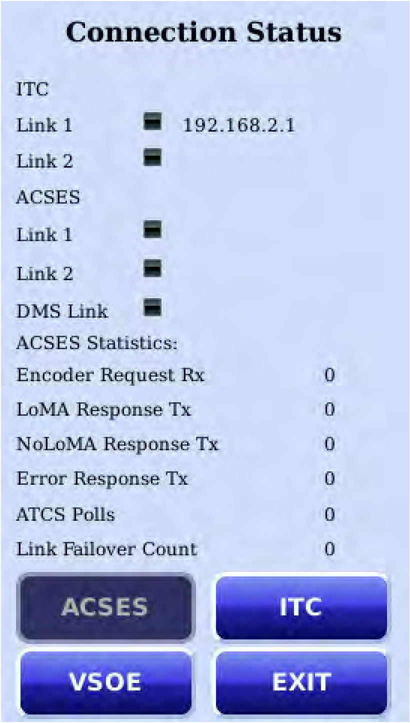
Step	Action
13	 Connection Status ITC Link 1 ■ 192.168.2.1 Link 2 ■ ACSES Link 1 ■ Link 2 ■ DMS Link ■ ACSES Statistics: Encoder Request Rx 0 LoMA Response Tx 0 NoLoMA Response Tx 0 Error Response Tx 0 ATCS Polls 0 Link Failover Count 0 Select the desired status, ***ACSES***, ***ITC,*** or ***VSOE***. Select ***EXIT*** to return to the Status screen.
14	To display the event log, select the ***LOG*** button.

Table 4–5. Accessing the System Screen (Cont.)

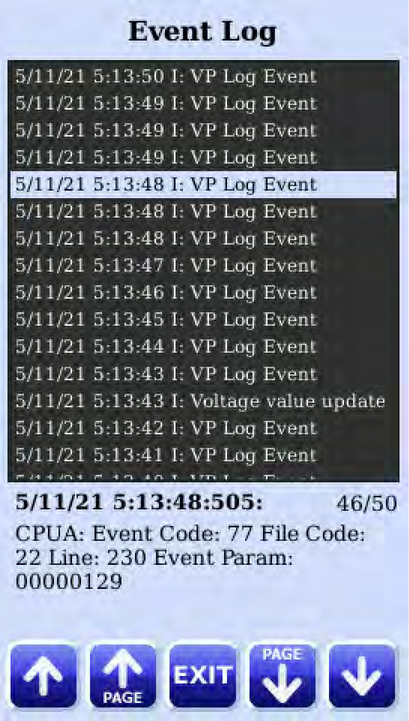
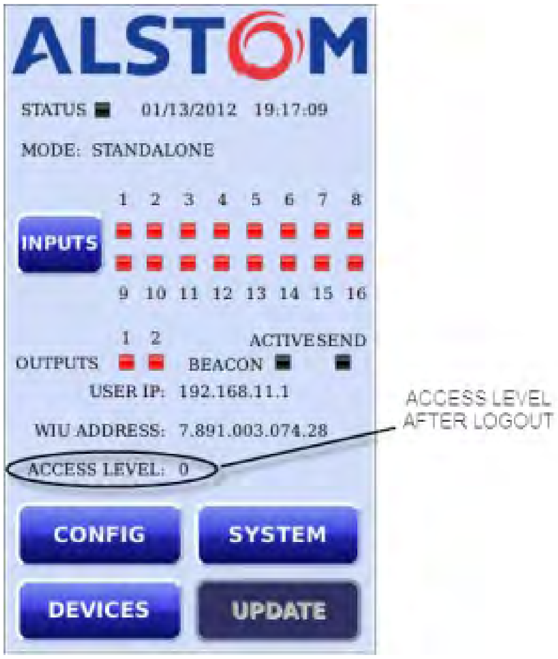
Step	Action
15	 Event Log 5/11/21 5:13:50 I: VP Log Event 5/11/21 5:13:49 I: VP Log Event 5/11/21 5:13:49 I: VP Log Event 5/11/21 5:13:49 I: VP Log Event 5/11/21 5:13:48 I: VP Log Event 5/11/21 5:13:48 I: VP Log Event 5/11/21 5:13:48 I: VP Log Event 5/11/21 5:13:47 I: VP Log Event 5/11/21 5:13:46 I: VP Log Event 5/11/21 5:13:45 I: VP Log Event 5/11/21 5:13:44 I: VP Log Event 5/11/21 5:13:43 I: VP Log Event 5/11/21 5:13:43 I: Voltage value update 5/11/21 5:13:42 I: VP Log Event 5/11/21 5:13:41 I: VP Log Event **5/11/21 5:13:48:505:** 46/50 CPUA: Event Code: 77 File Code: 22 Line: 230 Event Param: 00000129 Scroll through the log list using the arrow buttons. ***EXIT*** returns to the Status screen.
16	To log the current user out of the microWIU, select the ***LOGOUT*** button.

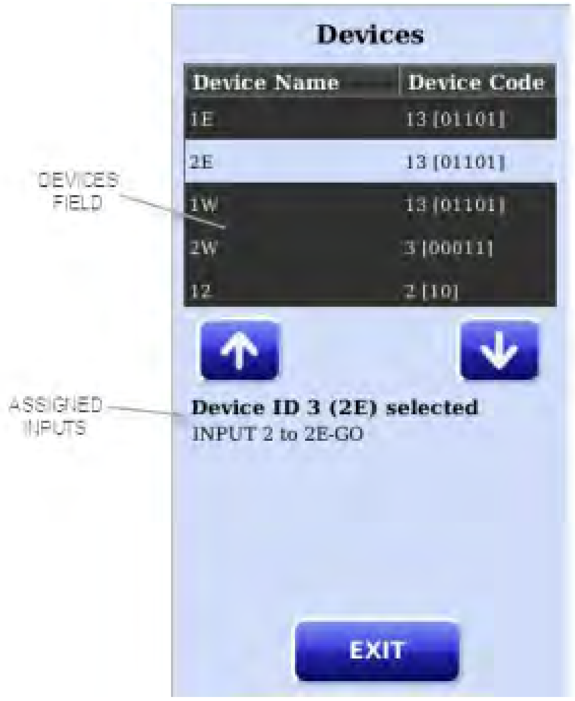
Table 4–5. Accessing the System Screen (Cont.)

Step	Action
17	The user is logged out and the Status screen reopens. The Access Level is reset to 0 (read-only access).  STATUS ■ 01/13/2012 19:17:09 MODE: STANDALONE USER IP: 192.168.11.1 WIU ADDRESS: 7.891.003.074.28 ACCESS LEVEL: 0 ACCESS LEVEL AFTER LOGOUT ALSTOM INPUTS 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 OUTPUTS 1 2 BEACON ACTIVE SEND CONFIG SYSTEM DEVICES UPDATE
18	To return to the Status screen, select the ***EXIT*** button.

4.4.5 Devices Screen

The ***DEVICES*** button on the Status screen displays the real-time value of the ITC Device Code for each ITC device monitored by the microWIU.

Table 4–6. Accessing the Devices Screen

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>From the Status screen, select the <b><i>DEVICES</i></b> button.
Note: If not already logged in, the Enter Passcode screen opens. See Step 2 in Table 4–4 for passcode entry instructions.</td></tr>
<tr><td>2</td><td><i>The Devices screen opens.</i>

Devices<table><tr><th>Device Name</th><th>Device Code</th></tr><tr><td>1E</td><td>13 [01101]</td></tr><tr><td>2E</td><td>13 [01101]</td></tr><tr><td>1W</td><td>13 [01101]</td></tr><tr><td>2W</td><td>3 [00011]</td></tr><tr><td>12</td><td>2 [10]</td></tr></table>Device ID 3 (2E) selected
INPUT 2 to 2E-GO

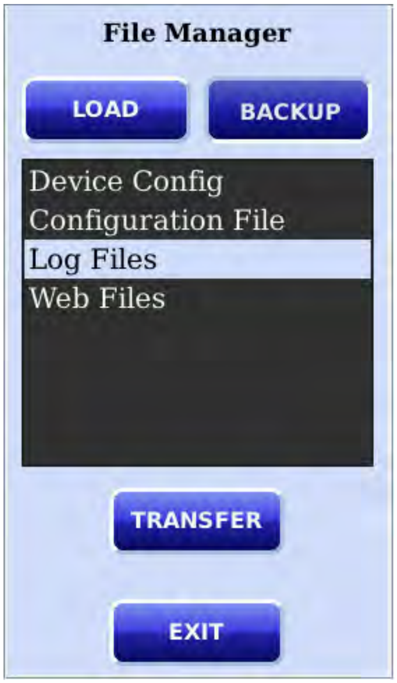
The Devices screen shows the device name and associated device code in the Devices field. When a device is selected, assigned inputs and outputs are displayed below the Devices field.
To scroll through the list of devices, use the UP/DOWN arrows.
When done, select the <b><i>EXIT</i></b> button.
Note: Device Codes display as [XXXXX] until beaconing becomes enabled</td></tr>
</table>

4.4.6 File Manager Screen

The ***UPDATE*** button on the Status screen displays the File Manager screen. The ***UPDATE*** button becomes active only when a USB device is inserted into the front panel of the microWIU. The USB device must contain the file types that the WIU uses to update configuration or executable files. Qualified personnel can use the File Manager screen to update configuration or executable files.

> Note: The functions on the File Manager screen are only to be performed by qualified personnel.

Table 4–7. Accessing the File Manager Screen

Step	**Action**
1	From the Status screen, select the ***UPDATE*** button.
2	*The File Manager screen opens, by default, with the Load button active.*  File Manager LOAD BACKUP Device Config Configuration File Log Files Web Files TRANSFER EXIT
3	To Update an application or the operating software, select the desired file (by clicking with the mouse for web interface or using the touch screen on the unit). Select ***TRANSFER*** to begin the update.
3a	To Backup files, select the ***BACKUP*** button. Highlight the desired file (by clicking with the mouse for the web interface or using the touch screen on the unit). Select ***TRANSFER*** to begin the file backup.
4	When done, select ***EXIT*** to return to the Status screen.

SECTION 5 – SOFTWARE UPDATES

Refer to Appendix B and Appendix C for additional application data details.

5.1 LOCAL SOFTWARE UPDATE

When a USB device is inserted into the front panel USB port of the microWIU, the unit checks that no changes have been made to the currently installed application or operating system software.

If the two software versions are not identical, the display acknowledges the software discrepancy and proceeds to initiate a software update. See Table 5-1 for the software update procedure.

WARNING

Prior to software installation, validation testing must confirm all application logic is correct.

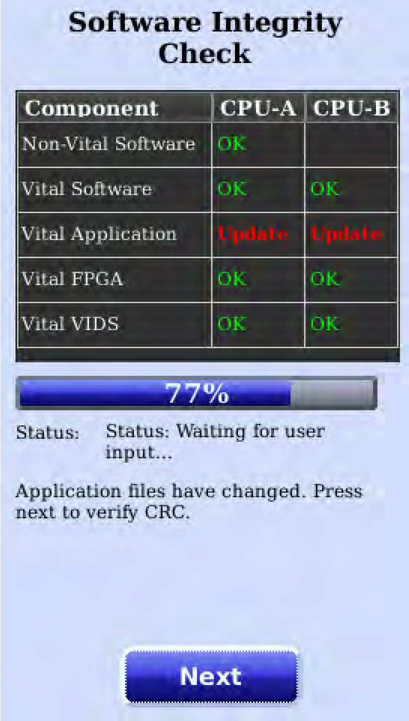
CAUTION

Applications created with a previous version of ADT software (i.e., different than the microWIU is currently running) need to be recompiled with the version of ADT software that matches the version on the target microWIU. Applications compiled in an older ADT version will render the microWIU nonfunctional.

Table 5-1. Local Software Update Procedure

<table>
<tr><th>Step</th><th>Procedure</th></tr>
<tr><td>1</td><td>Verify the USB device’s label is consistent with the correct site-specific application for transfer onto the microWIU.</td></tr>
<tr><td>2</td><td>Record results on Table B-1, Line 2.</td></tr>
<tr><td>3</td><td>Insert programmed USB device into front USB port J11.</td></tr>
<tr><td>4</td><td>

The microWIU checks for identical software versions between the unit and the programmed USB device.



Software Integrity Check

<table>
<tr><th>Component</th><th>CPU-A</th><th>CPU-B</th></tr>
<tr><td>Non-Vital Software</td><td>OK</td><td></td></tr>
<tr><td>Vital Software</td><td>OK</td><td>OK</td></tr>
<tr><td>Vital Application</td><td>Update</td><td>Update</td></tr>
<tr><td>Vital FPGA</td><td>OK</td><td>OK</td></tr>
<tr><td>Vital VIDS</td><td>OK</td><td>OK</td></tr>
</table>

77%

Status: Status: Waiting for user input...

Application files have changed. Press next to verify CRC.

Select ***Next***.

</td></tr>
</table>

Table 5-1. Local Software Update Procedure (Cont.)

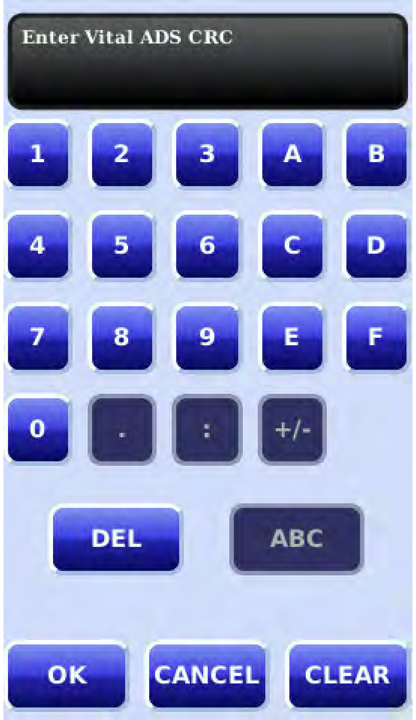
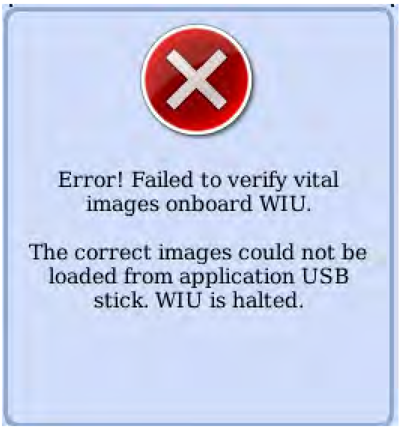
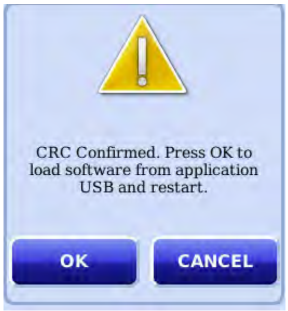
Step	Procedure
5	 Enter Vital ADS CRC 1 2 3 A B 4 5 6 C D 7 8 9 E F 0 . : +/- DEL ABC OK CANCEL CLEAR Enter the applicable CRC(s). Select ***OK***. Note: Using the remote web viewer is the easiest way to enter the CRCs.
6	 Error! Failed to verify vital images onboard WIU. The correct images could not be loaded from application USB stick. WIU is halted. If CRCs do not match, execution of the application is halted. User must investigate the cause of discrepancy (by re-entering the CRCs or re-validating the application) and correct before continuing.

Table 5-1. Local Software Update Procedure (Cont.)

Step	Procedure
6a	 CRC Confirmed. Press OK to load software from application USB and restart. When CRCs are confirmed identical, select ***OK*** to load application software.
7	Record results on Table B-1, Line 3.
8	When installation is finished, the microWIU restarts and the Status screen appears on the microWIU display.
9	Record results on Table B-1, Line 4.
10	Verify the network configuration is correct per site-specific Book of Plans.
11	Record results on Table B-1, Line 5.
12	Perform field testing of the Application before placing the location into revenue service, by following the testing plan and safety plan testing requirements for the Application.
13	Record results on Table B-1, Line 6.

5.2 REMOTE SOFTWARE UPDATE

WARNING

Prior to software installation, validation testing must confirm all application logic is correct.

Table 5-2. Remote Software Update Procedure

Step	Procedure
1	From a PC containing the ADT program, launch a web browser. Note: Java™ SE Runtime Environment, minimum version 7, must be installed on the PC. This software is freely available from Oracle at http://www.oracle.com/technetwork/java/javase/downloads/index.html.
2	Enter the following in the address bar: https://192.168.10.1/.

Table 5-2. Remote Software Update Procedure (Cont.)

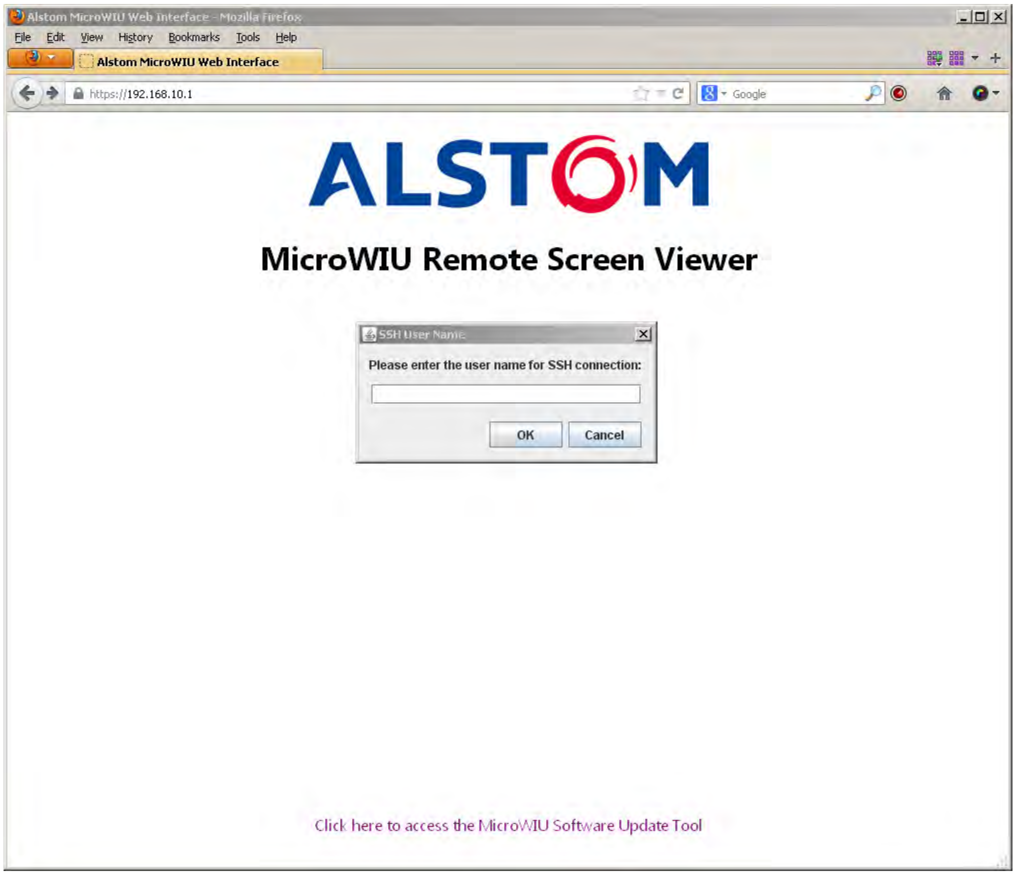
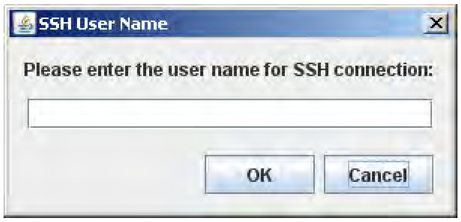
Step	Procedure
3	*The Alstom MicroWIU Remote Screen Viewer window opens.*  Alstom MicroWIU Web Interface - Mozilla Firefox File Edit View History Bookmarks Tools Help Alstom MicroWIU Web Interface https://192.168.10.1 Google ALSTOM SSH User Name OK Cancel MicroWIU Remote Screen Viewer Please enter the user name for SSH connection: Click here to access the MicroWIU Software Update Tool
3a	*The SSH User Name window also opens.*  Please enter the user name for SSH connection: Enter **microwiu**. Note: Username is case sensitive. Select ***OK***.

Table 5-2. Remote Software Update Procedure (Cont.)

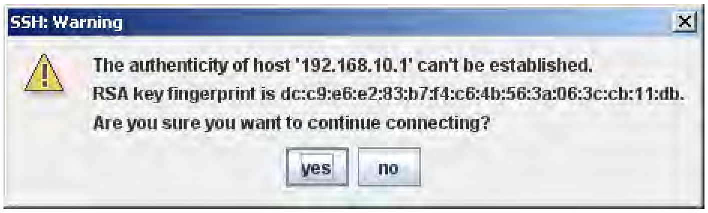
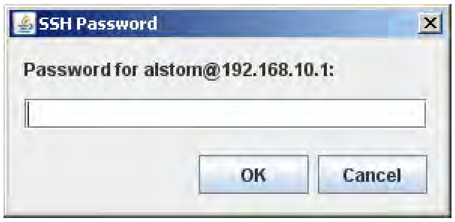
Step	Procedure
4	*The SSH Warning window opens.*  SSH: Warning The authenticity of host '192.168.10.1' can't be established. RSA key fingerprint is dc:c9:e6:e2:83:b7:f4:c6:4b:56:3a:06:3c:cb:11:db. Are you sure you want to continue connecting? Select ***YES***.
5	*The SSH Password window opens.*  SSH Password Password for alstom@192.168.10.1: Enter the microWIU System Password as set in the ADT ***Application Settings | Security*** tab.

Table 5-2. Remote Software Update Procedure (Cont.)

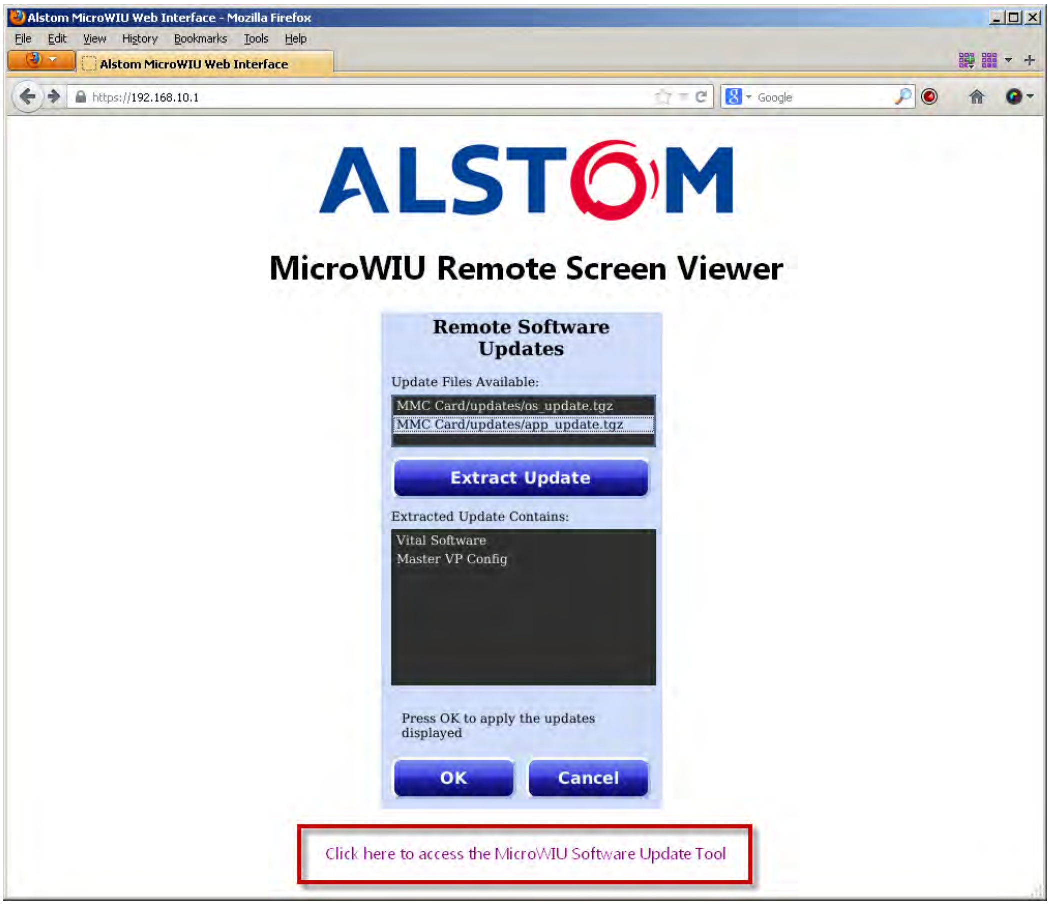
Step	Procedure
6	 Alstom MicroWIU Web Interface - Mozilla Firefox File Edit View History Bookmarks Tools Help Alstom MicroWIU Web Interface https://192.168.10.1 Google ALSTOM Extract Update OK Cancel MicroWIU Remote Screen Viewer Remote Software Updates Update Files Available: MMC Card/updates/os_update.tgz MMC Card/updates/app_update.tgz Extracted Update Contains: Vital Software Master VP Config Press OK to apply the updates displayed Click here to access the MicroWIU Software Update Tool Click the line that states ***Click here to access the MicroWIU Software Update Tool.***

Table 5-2. Remote Software Update Procedure (Cont.)

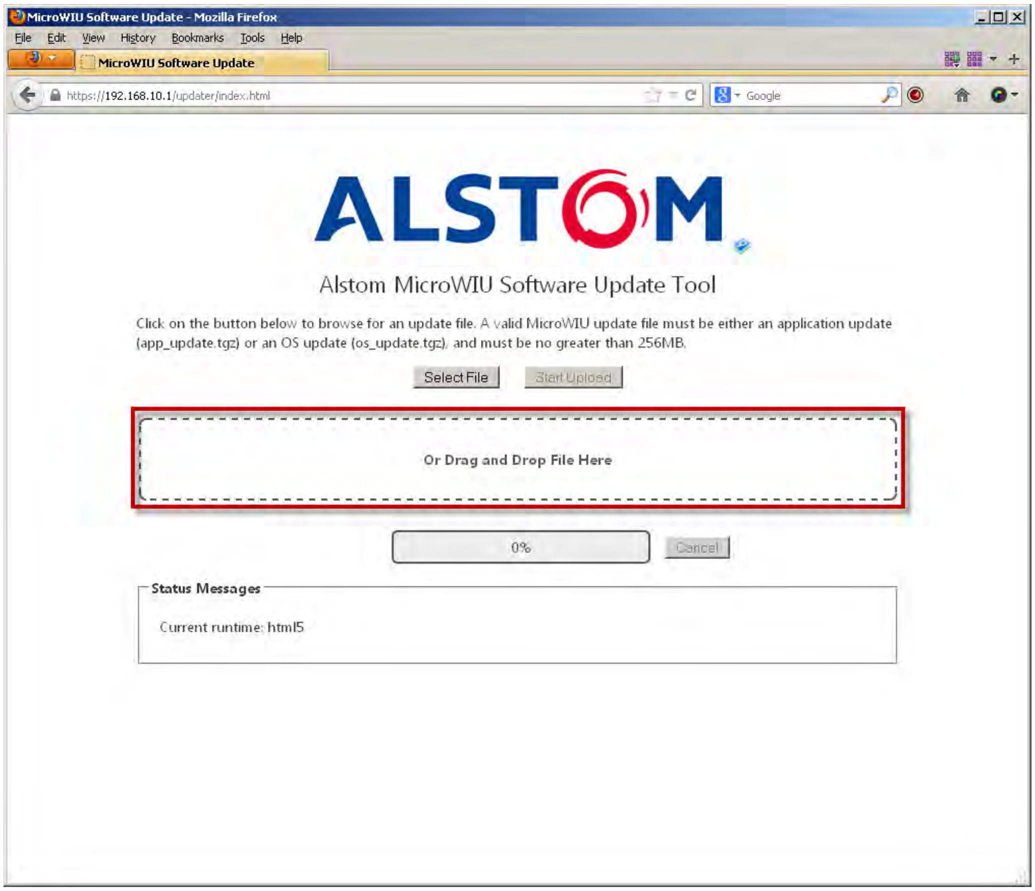
Step	Procedure
7	 MicroWIU Software Update - Mozilla Firefox File Edit View History Bookmarks Tools Help MicroWIU Software Update https://192.168.10.1/updater/index.html Google ALSTOM Select File Start Upload Or Drag and Drop File Here 0% Cancel Status Messages Alstom MicroWIU Software Update Tool Click on the button below to browse for an update file. A valid MicroWIU update file must be either an application update (app_update.tgz) or an OS update (os_update.tgz), and must be no greater than 256MB. Current runtime: html5 **Option 1:** Drag the (app_update.tgz) or an OS update (os_update.tgz) file into the Drag and Drop File Here area.

Table 5-2. Remote Software Update Procedure (Cont.)

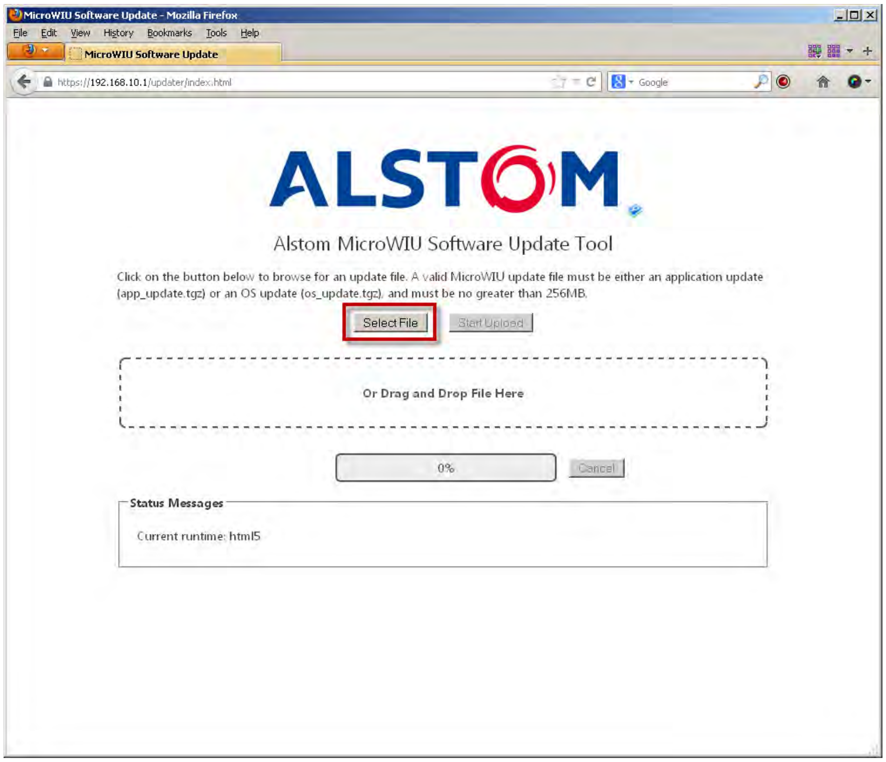
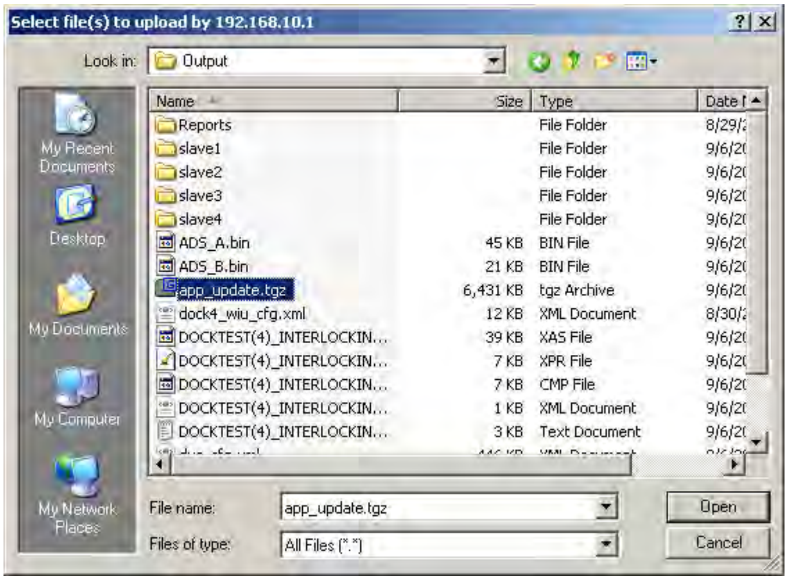
Step	Procedure
7a	 MicroWIU Software Update - Mozilla Firefox https://192.168.10.1/updater/index.html Alstom MicroWIU Software Update Tool Click on the button below to browse for an update file. A valid MicroWIU update file must be either an application update (app_update.tgz) or an OS update (os_update.tgz), and must be no greater than 256MB. Or Drag and Drop File Here 0% Status Messages Current runtime: html5 File Edit View History Bookmarks Tools Help MicroWIU Software Update Google Select File Start Upload Cancel  Select file(s) to upload by 192.168.10.1 Look in: Output Name / Size / Type / Date M Reports / / File Folder / 8/29/2 slave1 / / File Folder / 9/6/20 slave2 / / File Folder / 9/6/20 slave3 / / File Folder / 9/6/20 slave4 / / File Folder / 9/6/20 ADS_A.bin / 45 KB / BIN File / 9/6/20 ADS_B.bin / 21 KB / BIN File / 9/6/20 app_update.tgz / 6,431 KB / tgz Archive / 9/6/20 dock4_wiu_cfg.xml / 12 KB / XML Document / 8/30/2 DOCKTEST(4)_INTERLOCKIN... / 39 KB / XAS File / 9/6/20 DOCKTEST(4)_INTERLOCKIN... / 7 KB / XPR File / 9/6/20 DOCKTEST(4)_INTERLOCKIN... / 7 KB / CMP File / 9/6/20 DOCKTEST(4)_INTERLOCKIN... / 1 KB / XML Document / 9/6/20 DOCKTEST(4)_INTERLOCKIN... / 3 KB / Text Document / 9/6/20 File name: app_update.tgz Files of type: All Files (*.*) My Recent Documents Desktop My Documents My Computer My Network Places Open Cancel **Option 2:** Select ***Select File***. Browse to the Application update (app_update.tgz) or OS update (os_update.tgz) file to upload. Select ***Open***.

Table 5-2. Remote Software Update Procedure (Cont.)

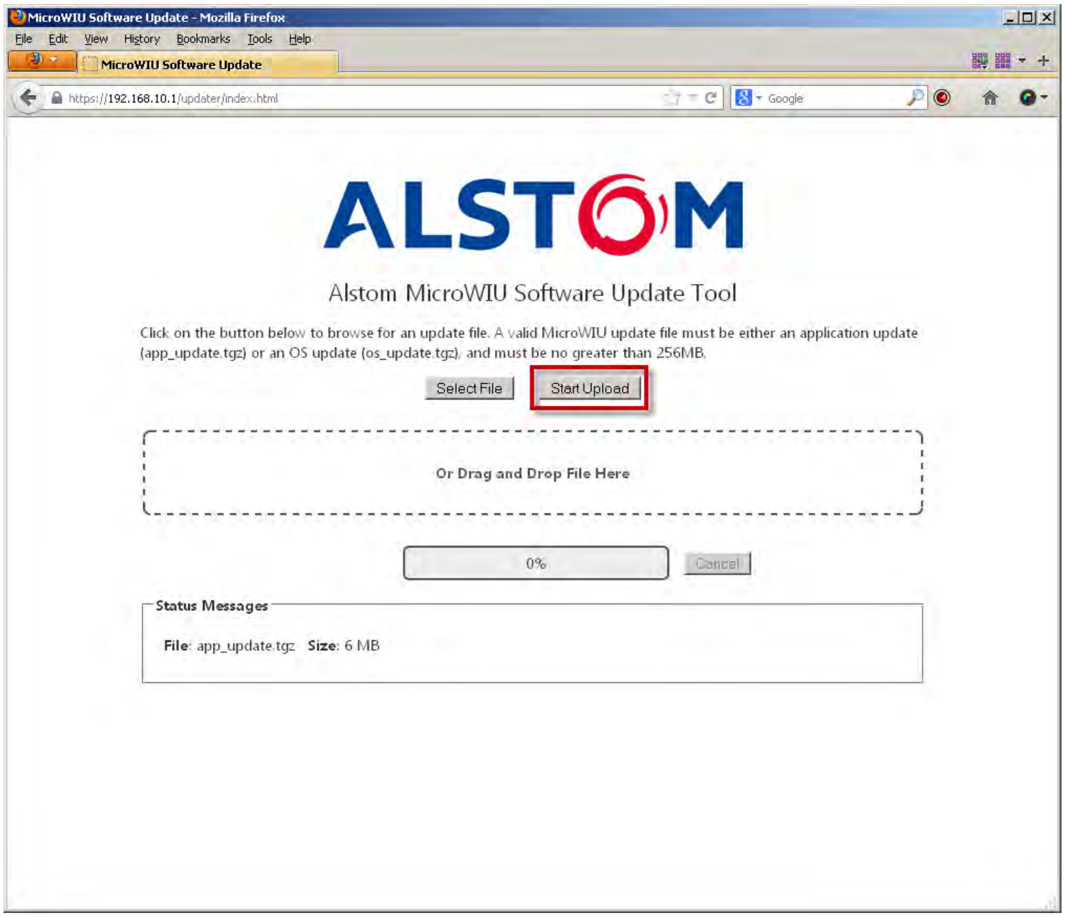
Step	Procedure
8	 MicroWIU Software Update - Mozilla Firefox File Edit View History Bookmarks Tools Help MicroWIU Software Update https://192.168.10.1/updater/index.html Google ALSTOM Select File Start Upload Cancel Alstom MicroWIU Software Update Tool Click on the button below to browse for an update file. A valid MicroWIU update file must be either an application update (app_update.tgz) or an OS update (os_update.tgz), and must be no greater than 256MB. Or Drag and Drop File Here 0% Status Messages **File**: app_update.tgz **Size**: 6 MB Select ***Start Upload***.

Table 5-2. Remote Software Update Procedure (Cont.)

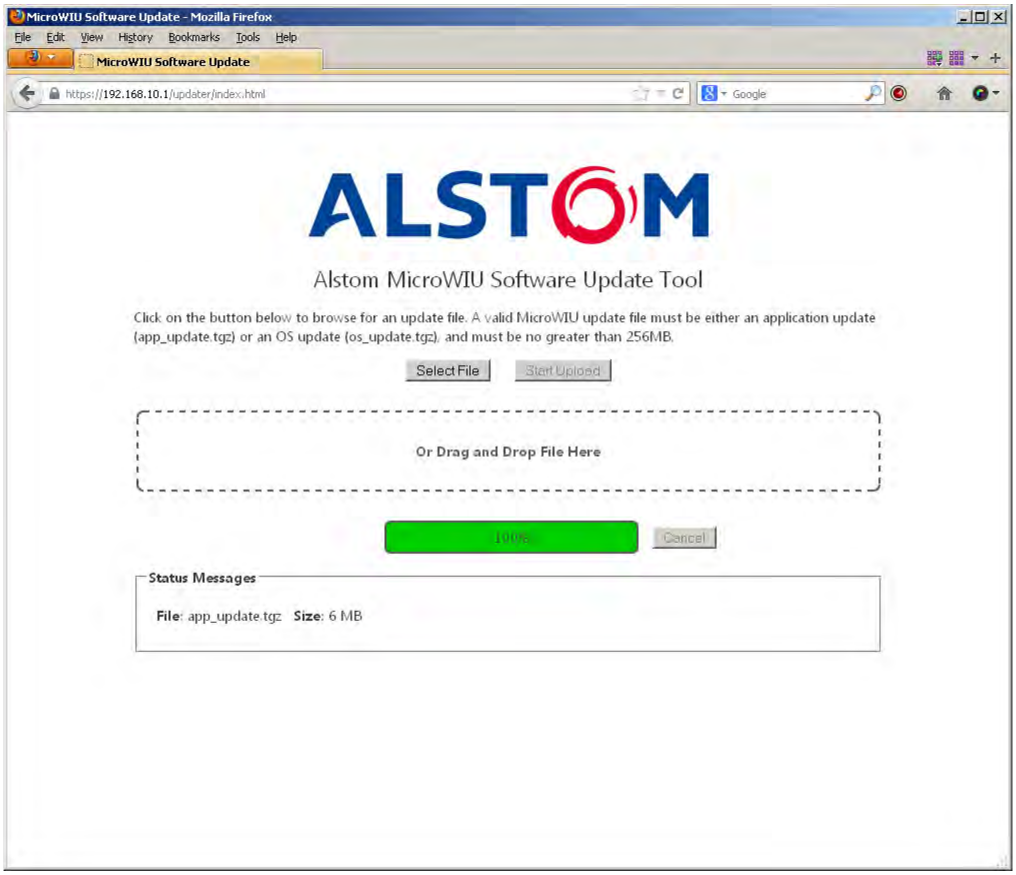
Step	Procedure
9	 MicroWIU Software Update - Mozilla Firefox File Edit View History Bookmarks Tools Help MicroWIU Software Update https://192.168.10.1/updater/index.html Google ALSTOM Select File Start Upload Or Drag and Drop File Here 100% Cancel Status Messages Alstom MicroWIU Software Update Tool Click on the button below to browse for an update file. A valid MicroWIU update file must be either an application update (app_update.tgz) or an OS update (os_update.tgz), and must be no greater than 256MB. **File**: app_update.tgz **Size**: 6 MB Once upload is complete, press the ***Confirm*** button on the Master or Standalone microWIU for one second.
10	Repeat Steps 2-5 to establish a connection again with the microWIU.

Table 5-2. Remote Software Update Procedure (Cont.)

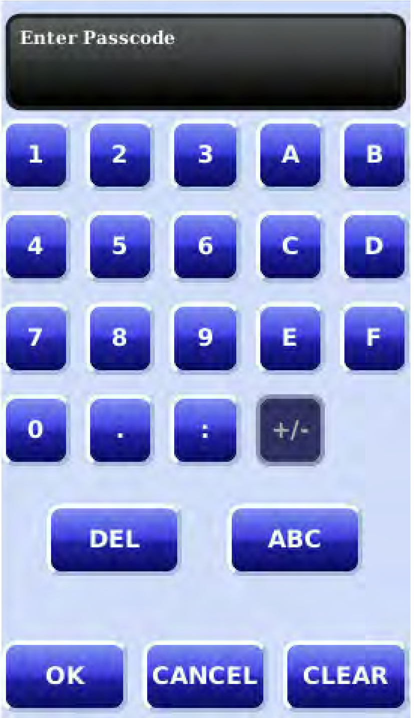
Step	Procedure
11	*MicroWIU screen is displayed, requiring a passcode to continue.*  Enter Passcode 1 2 3 A B 4 5 6 C D 7 8 9 E F 0 . : +/- DEL ABC OK CANCEL CLEAR Enter the security level passcode (PIN) as established in the ADT application. Select ***OK***.

Table 5-2. Remote Software Update Procedure (Cont.)

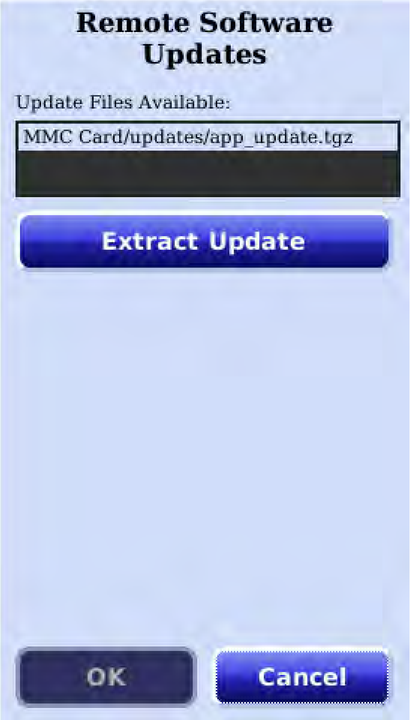
Step	Procedure
12	*A new window opens.*  Remote Software Updates Update Files Available: MMC Card/updates/app_update.tgz Select ***Extract Update***.

Table 5-2. Remote Software Update Procedure (Cont.)

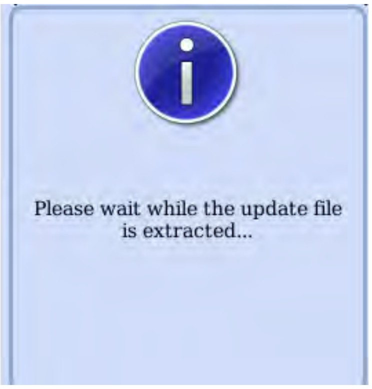
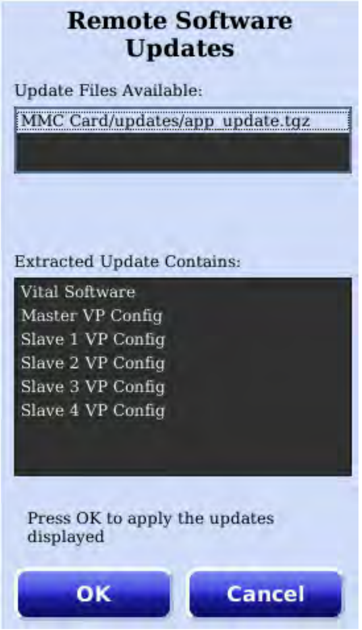
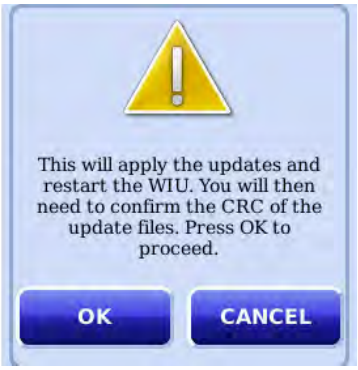
Step	Procedure
13	*The following windows open.*  Please wait while the update file is extracted...  **Remote Software Updates** Update Files Available: MMC Card/updates/app_update.tgz Extracted Update Contains: Vital Software Master VP Config Slave 1 VP Config Slave 2 VP Config Slave 3 VP Config Slave 4 VP Config Press OK to apply the updates displayed  This will apply the updates and restart the WIU. You will then need to confirm the CRC of the update files. Press OK to proceed. Select ***OK*** to apply the updates.

Table 5-2. Remote Software Update Procedure (Cont.)

Step	Procedure
14	When CRCs are confirmed identical, select ***OK*** to load application software.
15	Record results on Table B-1, Line 3.
16	When installation is finished, the microWIU restarts and the Status screen appears on the microWIU display.
17	Record results on Table B-1, Line 4.
18	Verify the network configuration is correct per site-specific Book of Plans.
19	Record results on Table B-1, Line 5.
20	Perform field testing of the Application before placing the location into revenue service, by following the testing plan and safety plan testing requirements for the Application.
21	Record results on Table B-1, Line 6.

SECTION 6 – TROUBLESHOOTING

6.1 INTRODUCTION

This section describes the troubleshooting of the microWIU. Troubleshooting helps to determine defective parts of equipment requiring repair or replacement. This is done through fault isolation diagrams and special instructions.

For ease of maintenance, diagnostic indications are included in the microWIU status LEDs. This gives maintenance personnel an indication that a failure has occurred.

WARNING

The microWIU must never be opened and/or serviced by anyone other than Alstom.

6.2 GENERAL TROUBLESHOOTING

General troubleshooting can be summarized as follows:

- Understand and define the problem
- Confirm the problem
- Isolate the fault
- Perform corrective action
- Verify system operation

Standard troubleshooting, such as verifying wiring and energy, can identify a failure. If the unit fails to operate at all (all LEDs off), check that the local energy is present at the corresponding plug board terminals.

Any unit that is suspected of being defective must be removed from service. If a microWIU is suspected to be defective, return the entire unit to Alstom Signaling for repair. Contact Alstom Signaling Inc. Customer Service at 1-800-717-4477 or www.alstomsignalingsolutions.com.

6.3 LEDS

The LEDs on the microWIU indicate if the internal circuitry of the unit is powered and the system software is executing correctly.

The three LEDs, visible from the front of the microWIU, are shown in Figure 2–1. The LEDs illuminate as follows:

- Power is lit GREEN when the unit is powered on
- Status is lit:
  - GREEN when the unit is operating normally (no warnings)
  - YELLOW when a warning condition has been detected, but the unit is operating (possibly in a degraded mode depending on the warning condition)
  - RED when an error condition has been detected and the unit is not operational
- Attention is lit RED when a condition exists that requires user attention

During the microWIU power-up sequence, the Status and Attention LEDs flash GREEN until the boot process is complete.

6.4 HARDWARE FAULT ERROR CODES

If operational faults are suspected or detected, the unit provides clear status information to isolate and repair the problem.

The microWIU displays the real-time Vital input state status (OFF, ON, Flashing) and log Vital input state transitions to a time-stamped event log.

The microWIU implements on-board logging of diagnostic information including (but not limited to) USB device access errors, file system errors, Vital hardware input circuit check failures, communications port failures, and internal processing errors.

Table 6–1. Hardware Failure Error Codes

Error	Description	Remedy
001	Class D Link Unable to Connect	Verify from warning message the port/IP address of the Class D connection, and then verify on the System screen that the network port is GREEN. • If the network port is GREEN, troubleshoot the Application Gateway • If the network port is not GREEN, troubleshoot the physical connection to the network for that port

SECTION 7 – CORRECTIVE MAINTENANCE

7.1 GENERAL

The microWIU is the Lowest Replaceable Unit. If the unit fails, it is replaced.

WARNING

The microWIU must never be opened and/or serviced by anyone other than Alstom.

WARNING

Certain replacement hardware is identified by unique keying of input connectors. Proper care needs to be given to ensure keying of new connectors matches those being replaced.

7.2 UNIT REMOVAL

Table 7–1. microWIU Removal

Step	Procedure
1	Verify the power switch on the unit to be replaced is in the OFF position, if applicable.
2	Remove input power from the unit.
3	Disconnect power and data cables from the unit (J1–J6).

Table 7–1. microWIU Removal (Cont.)

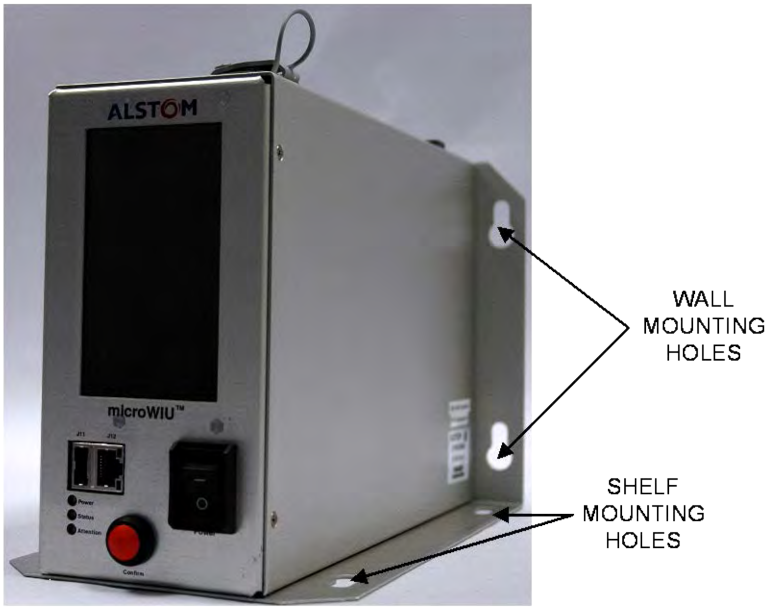
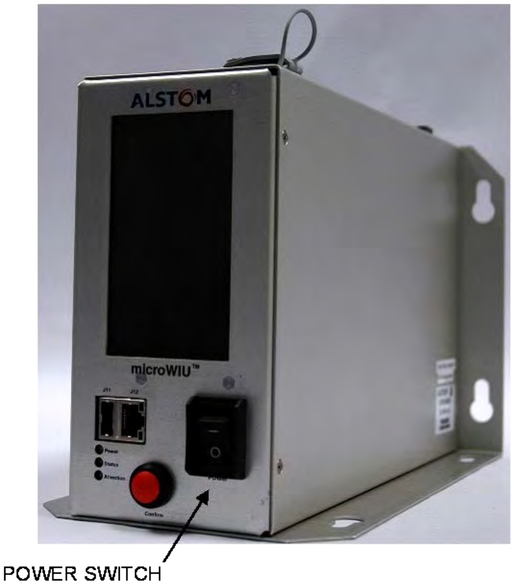
Step	Procedure
4	Remove the unit mounting hardware. See the site-specific Book of Plans, as required.  ALSTOM microWIU™ J11 J12 Power Status Attention Confirm WALL MOUNTING HOLES SHELF MOUNTING HOLES
5	Obtain a spare or replacement unit.
6	Verify the replacement microWIU power switch is in the OFF position, if applicable.  ALSTOM microWIU™ J11 J12 Power Status Attention Confirm POWER SWITCH

Table 7–1. microWIU Removal (Cont.)

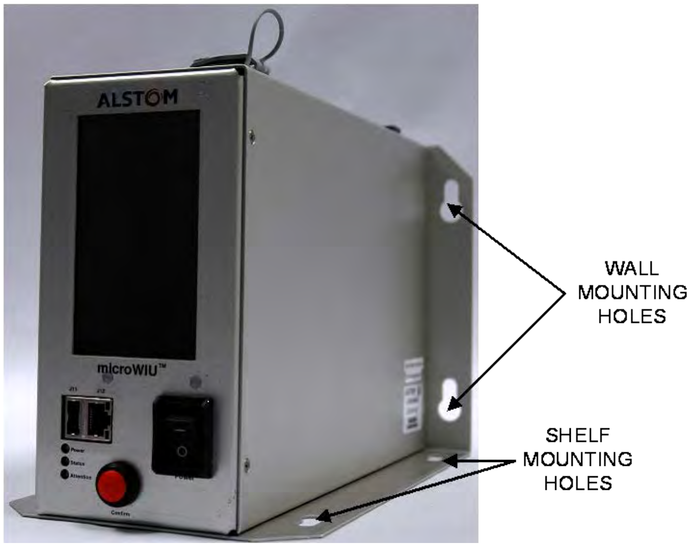
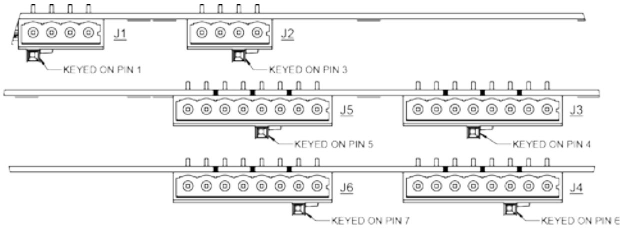
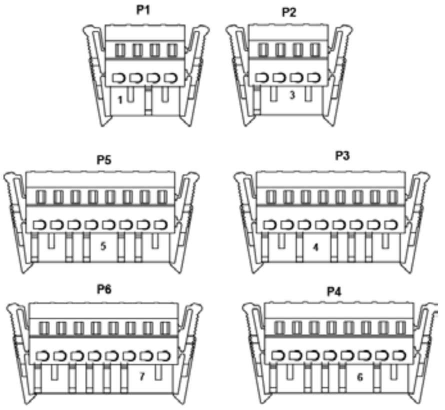
Step	Procedure
7	Using the mounting holes provided on the unit, install the appropriate mounting hardware. See the site-specific Book of Plans as required.  ALSTOM microWIU™ WALL MOUNTING HOLES SHELF MOUNTING HOLES

Table 7–1. microWIU Removal (Cont.)

Step	Procedure
8	For replacement receptacles, rekeying is necessary. Receptacles (P1-P6) are to be keyed to match plugs (J1-J6) respectively.  J1 KEYED ON PIN 1 J2 KEYED ON PIN 3 J5 KEYED ON PIN 5 J3 KEYED ON PIN 4 J6 KEYED ON PIN 7 J4 KEYED ON PIN 6 SHOWING KEYING LOCATIONS FOR RECEPTACLES (J1 THRU J6)  P1 1 P2 3 P5 5 P3 4 P6 7 P4 6 SHOWING KEYING PINS REMOVED FOR RECEPTACLES (P1 THRU P6) Rekey receptacles per diagram by breaking off keying tabs on receptacles. Refer also to Section 3.4.
9	Connect power, input, output, and data cables as specified in the site-specific Book of Plans.
10	Supply power to the unit. See the site-specific Book of Plans as required.
11	Turn the unit power switch to the ON position, if applicable. The Power and Status LEDs flash during the microWIU boot process.

SECTION 8 – PARTS CATALOG

This section identifies and lists the component parts that can be ordered to repair the Alstom microWIU at the shop level. The Lowest Replaceable Unit (LRU) for the microWIU is the unit itself. Individual parts are identified in Table 8–1.

Table 8–1. microWIU Parts List

Description	Figure No.	Alstom Part No.
microWIU (without Power Switch, with Cover)	Figure 8-1	41795-007-01
microWIU (With Power Switch)	Figure 8-2	41795-007-02
microWIU (without Power Switch)	Figure 8-3	41795-007-03
microWIU (without Power Switch)	Figure 8-3	41795-007-04
microWIU (without Power Switch, with B-2 width flange)	Figure 8-4	41795-007-05
ADT Software	N/A	51795-087-02
8-position Connector	Figure 8-5	58920-675-00
4-position Connector	Figure 8-5	58920-446-00
USB Memory Stick (USB device)	Figure 8-6	59522-165-00
Fuse	Figure 8-7	59524-046-00

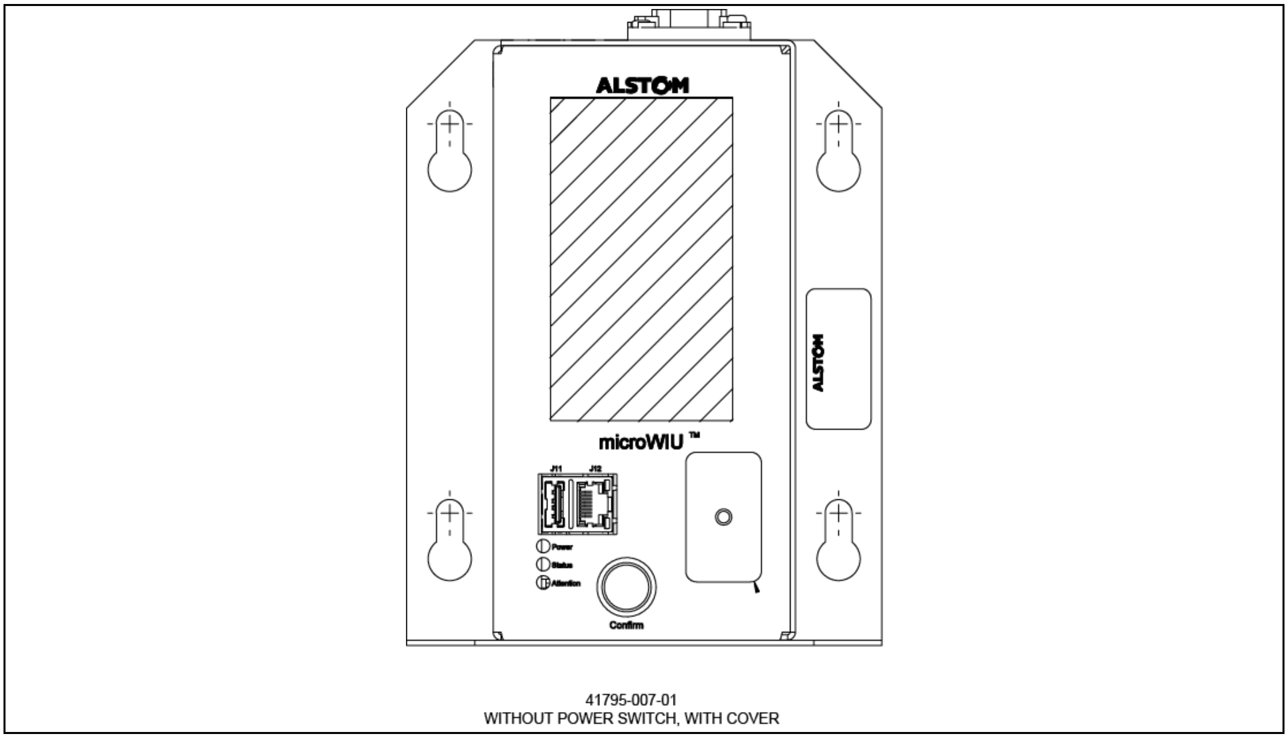


Figure 8-1. microWIU (without Power Switch, with Cover)

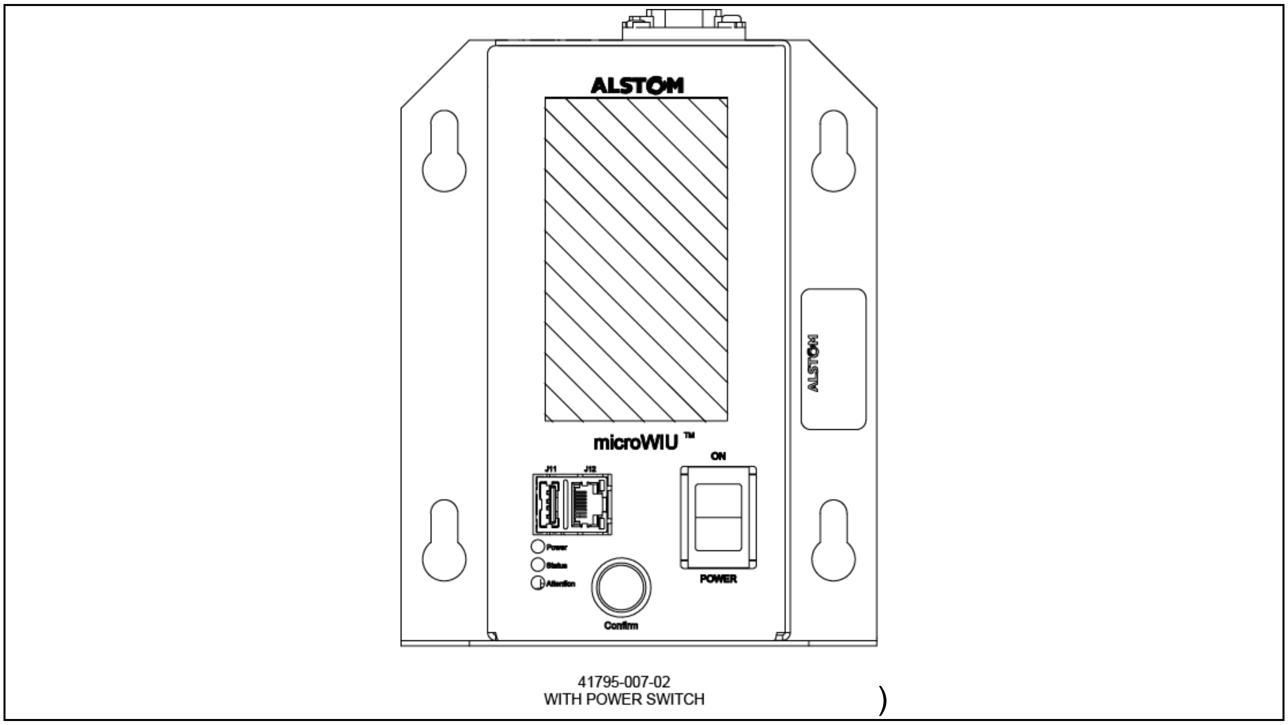
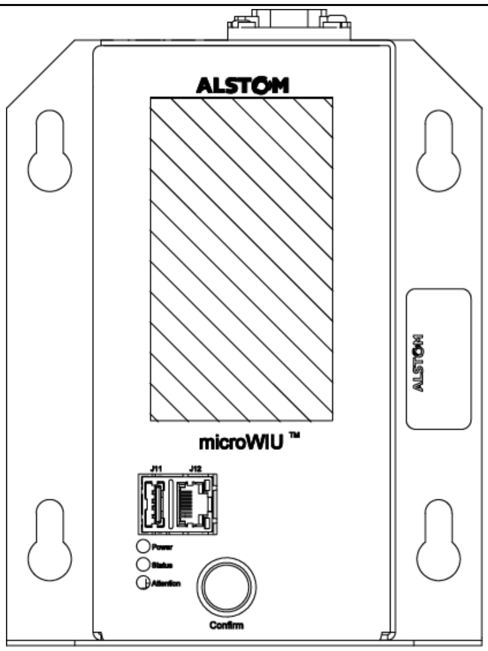
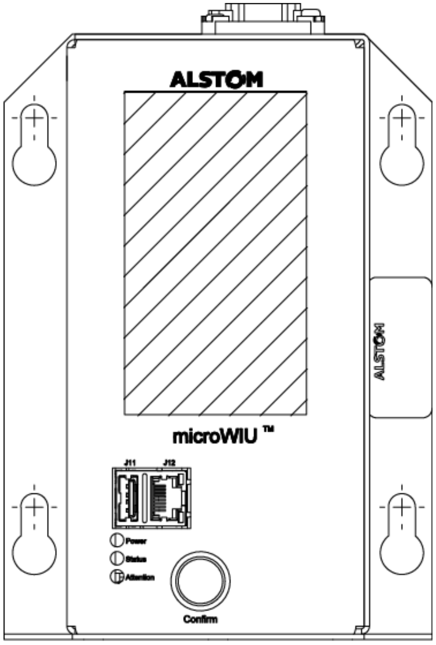


Figure 8-2. microWIU (With Power Switch)



41795-007-03, 41795-007-04
WITHOUT POWER SWITCH

Figure 8-3. microWIU (without Power Switch)



41795-007-05
WITHOUT POWER SWITCH, WITH B2-WIDTH FLANGE

Figure 8-4. microWIU (without Power Switch, with B-2 width flange)

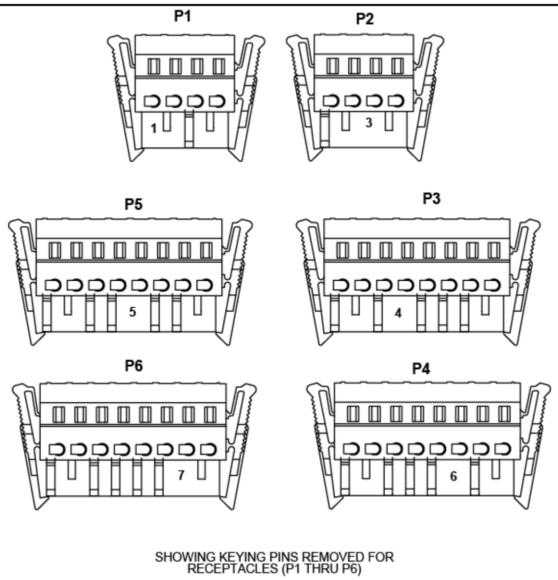


Figure 8-5. 8- and 4-Position Receptacles (with pins removed for keying)

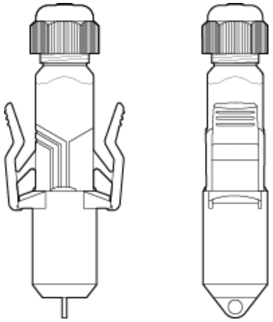


Figure 8-6. USB Memory Stick

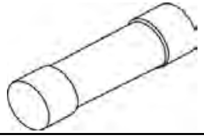


Figure 8-7. Fuse

APPENDIX A – TYPICAL APPLICATION CIRCUITS

A.1 APPLICATION CIRCUITS

WARNING

The microWIU Vital input circuits may activate with a minimum signal of 3.4 V and 10.2 milliamperes in worst case scenario under failure conditions.

To prevent a potential unsafe condition, any external voltage source attached to a microWIU Vital input circuit must generate less than 3.4 V and 10.2 milliamperes in worst case scenario under failure conditions when the device controlling the source voltage is in the de-energized state.

This requirement includes all environmental operating conditions and all operating values of the external voltage source over its service life, including worst case scenario under failure conditions. Failure to follow this requirement may lead to unexpected operation of the microWIU input circuit.

WARNING

The microWIU Vital input circuits may fail with a complete short between the input positive and negative terminals. To prevent a potential unsafe condition, this failure mode must be considered when the microWIU Vital input circuit is connected in parallel with any other load device (i.e., a signal lamp).

Failure to consider this failure mode may lead to unexpected operation of the microWIU input circuit in the event the Vital input shorts.

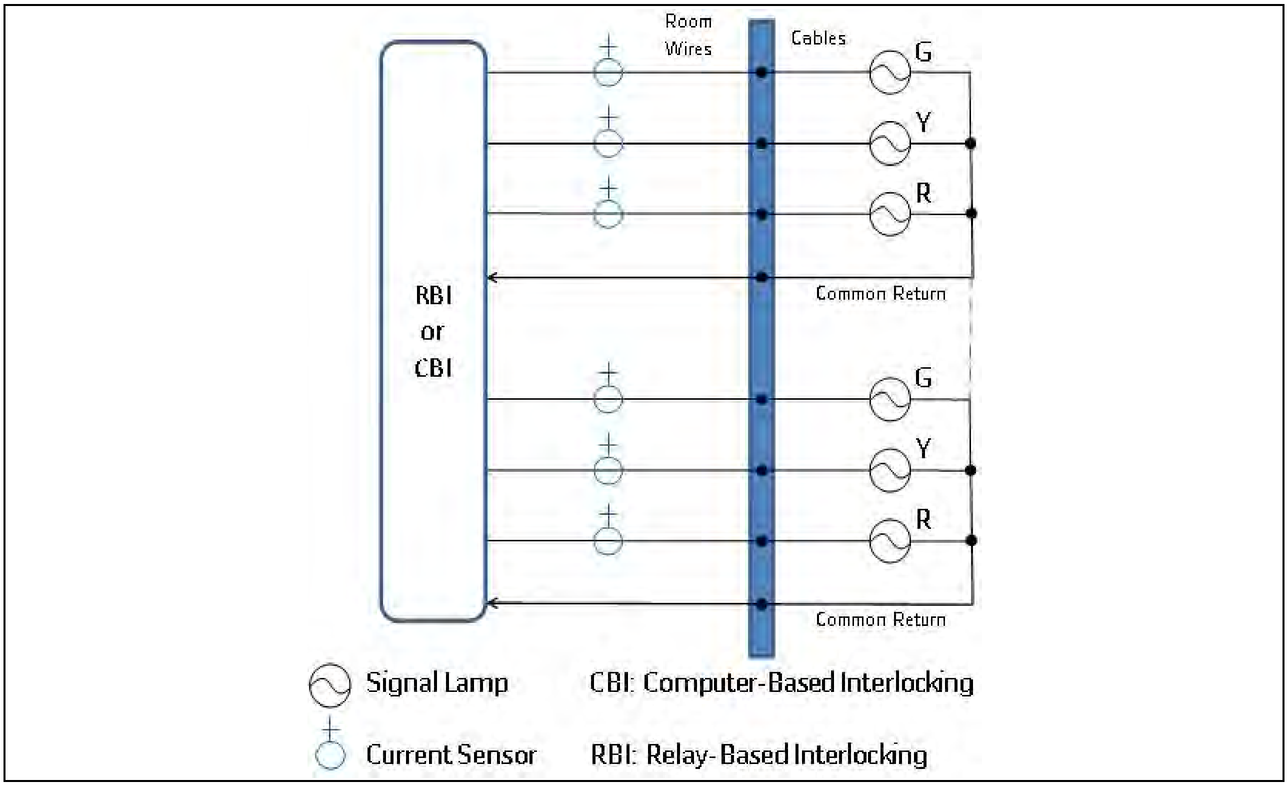


Figure A-1. Typical Color Light Application Circuit Using Current Sensors Only

- A single sensor is used to determine each lamp status.
- Each aspect needs one current sensor.
- Each current sensor connects to one microWIU input.
- Shared common return is allowed between signal heads.

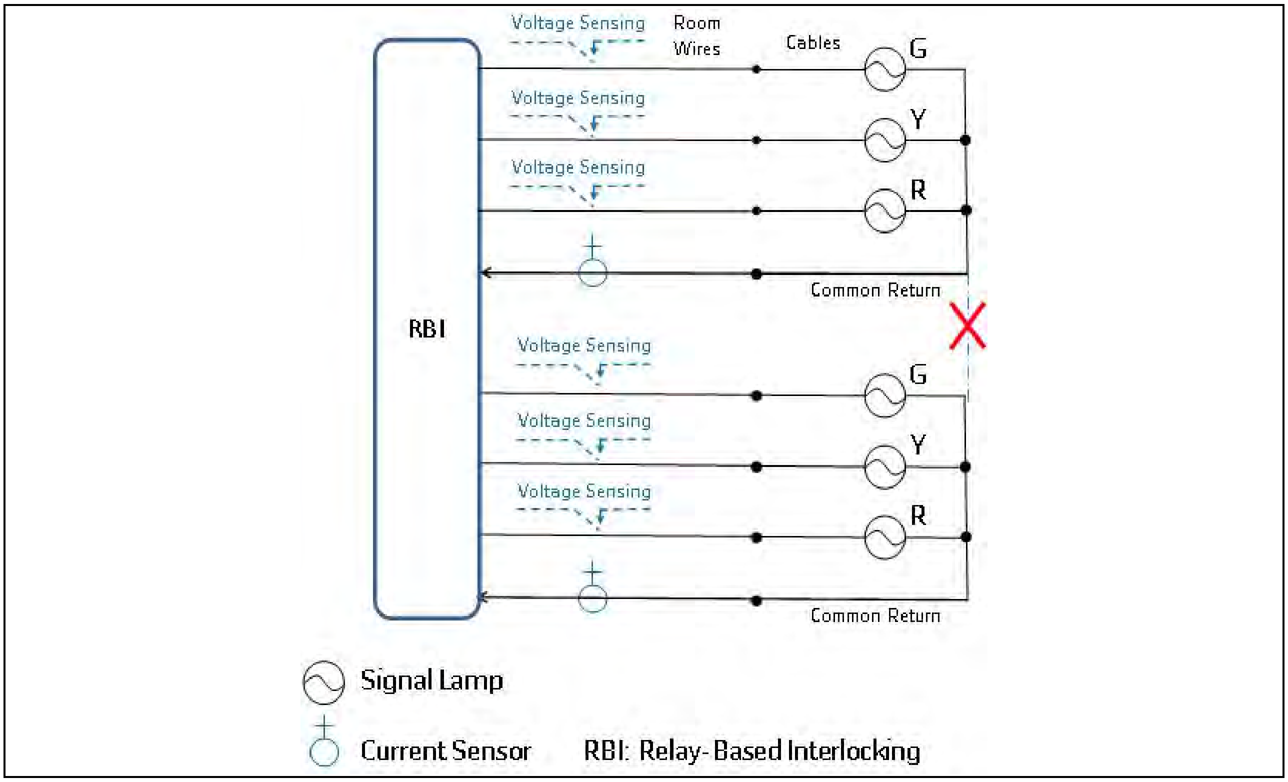


Figure A-2. Typical Color Light Application Circuit Using Current Sensors and Relay Contacts

- The microWIU uses voltage sensing combined with a single current sensor output to determine each lamp status.
- Each color light aspect and the common return needs one microWIU input for the voltage sensing and one microWIU input for the current sensing.
- No shared common return is allowed between signal heads.
- Voltage sensing is accomplished by a Vital relay contact closure, which shall be voltage-free if a Vital filament check is required. If this is not practical, a safety analysis must be performed case by case.

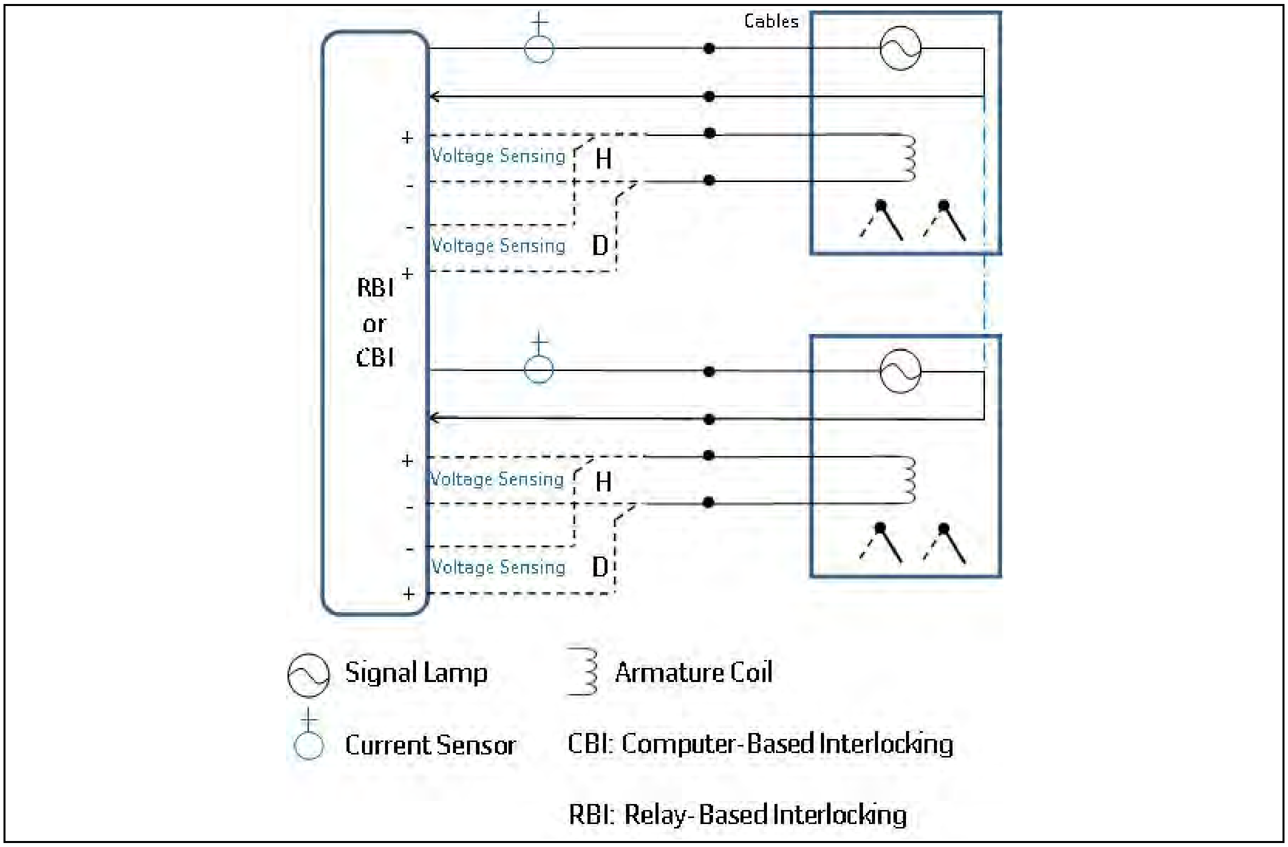


Figure A-3. Typical Search Light Application Circuit Using Current Sensors and Relay Contacts

- The microWIU uses a single sensor to determine the lamp status.
- Each lamp (head) needs one current sensor.
- Each current sensor connects to one microWIU input.
- Shared common return is allowed between signal heads.
- The armature drive is voltage-sensed with one microWIU input for each drive.

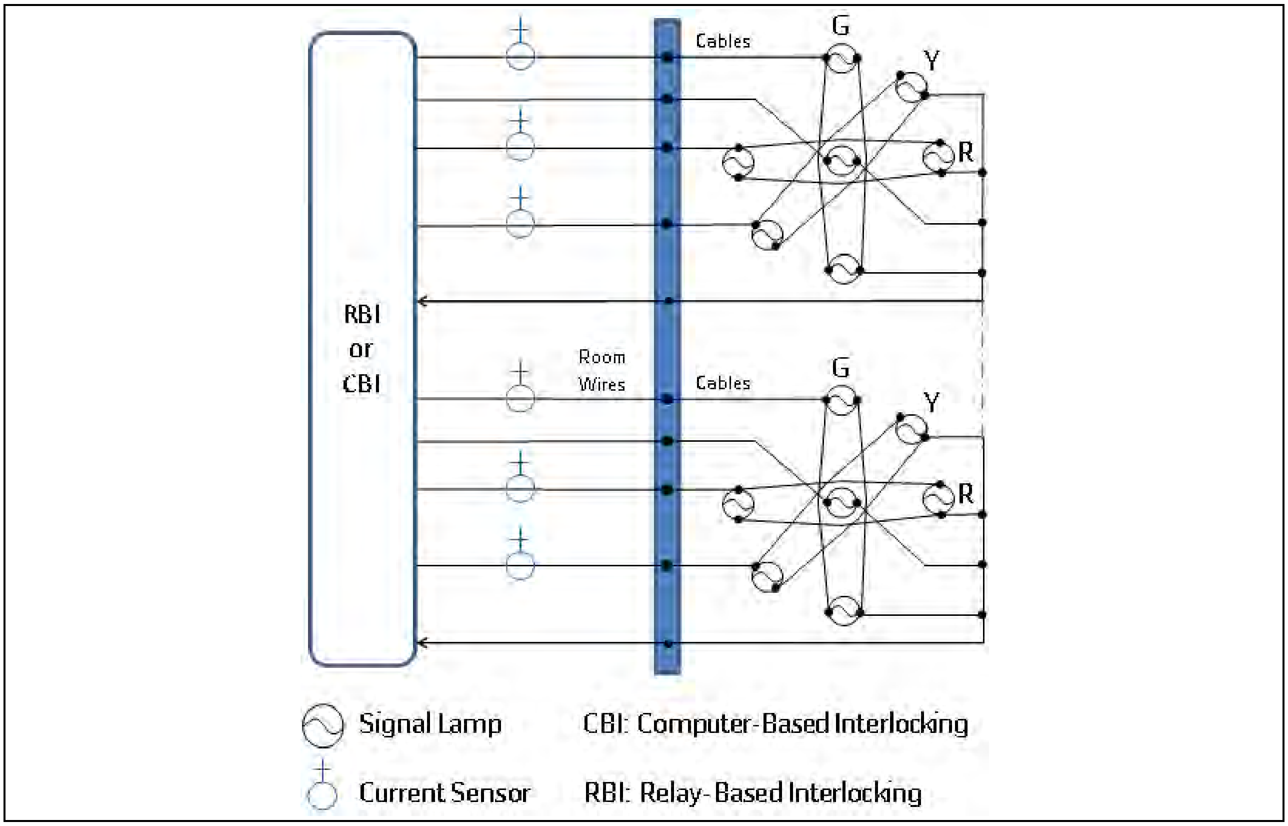

RBI
or
CBI
Room
Wires
Cables
Cables
G
Y
R
G
Y
R
Signal Lamp
Current Sensor
CBI: Computer-Based Interlocking
RBI: Relay-Based Interlocking

Figure A-4. Typical Color Position Light Application Circuit
Using Current Sensors Only

- The microWIU uses a single current sensor to determine each color aspect status.
- Each aspect needs one current sensor.
- Each current sensor connects to one microWIU input.
- Shared common return is allowed between signal heads.

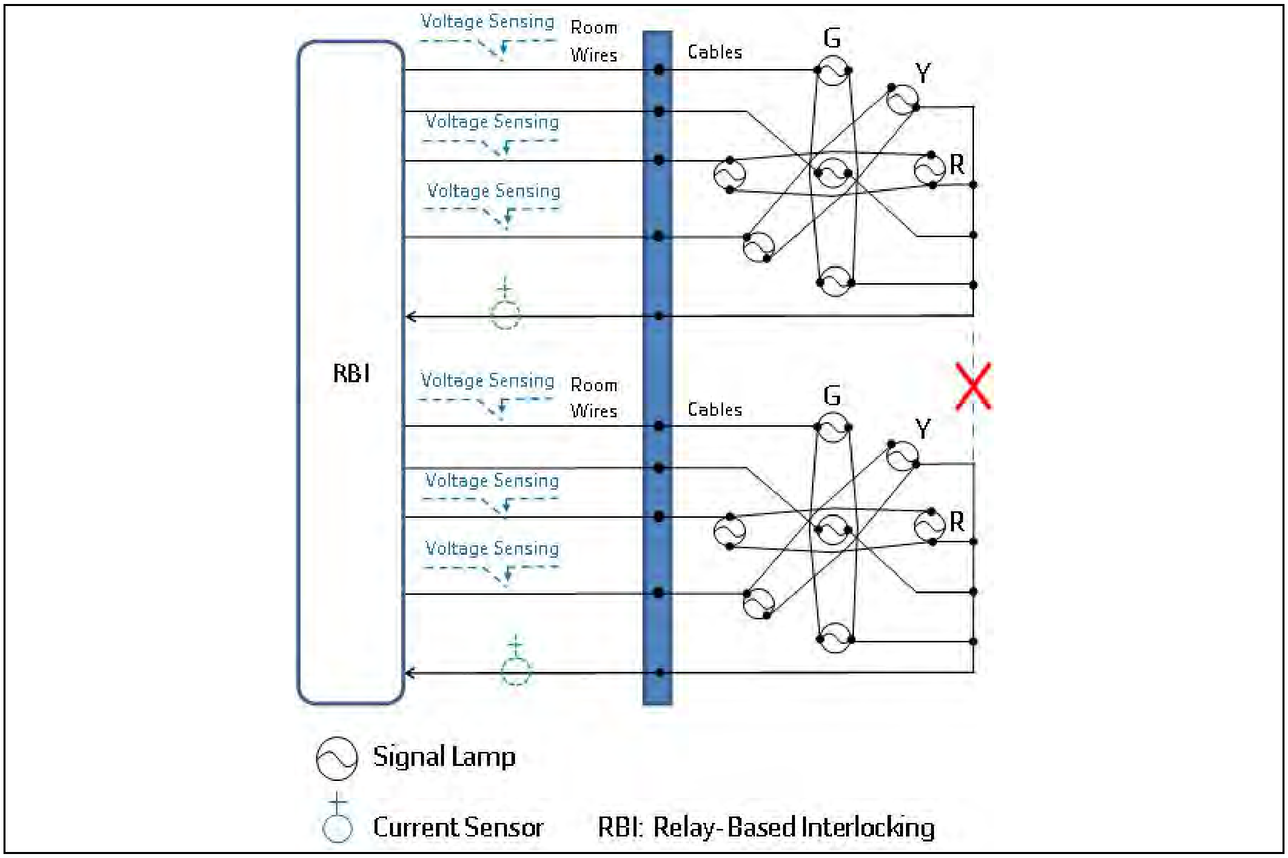


Figure A-5. Typical Color Position Light Application Circuit
Using Current Sensors and Relay Contacts

- The microWIU uses voltage sensing to determine each color aspect status. The current sensing is not necessary if it is assumed that the redundant lamps protect against a dark signal.
- Each color light aspect needs one microWIU input. A current sensor can be used which takes a microWIU input.
- No shared common return is allowed between signal heads if the current sensors are used.
- Voltage sensing is accomplished by a Vital relay contact closure, which shall be voltage-free in case of a short circuit across the lamps. If this is not practical, a safety analysis must be performed case by case.

APPENDIX B – PREPARATION PROCESS DATA SHEET

B.1 INTRODUCTION

This section contains the data sheet checklist to record all necessary preparation process steps required by the customer/railroad to validate information contained in the microWIU application before beginning revenue service.

Retain all data sheets for future reference in the location prescribed by the rules of the local governing authority.

Use this data sheet in conjunction with Section 3.3 and Section 5.

Table B-1. Application Validation Report Data Sheet

ALSTOM

Project Name: ______________________________

Project Location: ______________________________

ADT Version: ______________________________

CAA Version: ______________________________

ADV Version: ______________________________

Compile Date and Time: ______________________________

ADV Checker’s Name: ______________________________

Today’s Date: ______________________________

Comments: ______________________________

____

____

____

Table B-1. Application Validation Report Data Sheet (Cont.)

Line	Section	Action	Validated as Correct by
1	P2526 ADT User Manual, Section 6	A completed copy of *Table A–1. Application Validation Report Data Sheet* has been saved per governing authority rules.	
2	3.3.1, 3.3.2, 5.1, 5.2	Verify the USB device's label is consistent with the correct site-specific application to be transferred onto the microWIU (i.e., the correct application for the location).	
3	3.3.1, 3.3.2, 5.1, 5.2	Verify CRCs are all correct and no CRC errors received during application installation.	
4	3.3.1, 3.3.2, 5.1, 5.2	Verify application successfully installed.	
5	3.3.1, 3.3.2, 5.1, 5.2	Verify correct "as-built" microWIU network configuration, including VSOE2 configuration.	
6	3.3.1, 3.3.2, 5.1, 5.2	Validation field testing has been successfully completed, confirming all application logic is correct and consistent with application requirements.	

APPENDIX C – SAFETY-RELATED APPLICATION CONDITIONS / ACTIONS

This section contains the Safety-Related Application checklist to record all evidence required by the customer/railroad to validate information contained in the microWIU application before beginning revenue service.

Retain this checklist information for future reference in the location and format prescribed by the rules of the local governing authority.

Table C–1. Safety-Related Application Checklist

Safety-Related Application Condition Number	Responsible Personnel	Safety Related Application Conditions / Action	Evidence for Implementation
SRAC.1	Application Design Installation Maintenance	The ADT/CAA/ADV shall be exclusive to Alstom personnel only or skilled and trained Application Designers per contract according to uWIU manuals.	
		The verification and validation process using the ADV tool must ensure that the uWIU is programmed with the correct application logic and is correctly configured.	
		For each uWIU configured, a Consolidation Report or equivalent documentation, is requested in order to build evidence that: 1. Application Data Verification (ADV) is “Pass” 2. No unused input is linked to a valid WSM (in .xpr file) and VRM (in .xas file) output msg. (Manual check for BL3&4 and automatic check for BL5 by ADV). 3. CRC matches and is correct after download on USB plug.	
		Front panel check is requested: - “As built” verification of the correct uWIU Application and Firmware is activated (Revision, Revision Date and CRC associated), - “As built” verification of the correct uWIU network configuration (including VSOE2 configuration for product BL5). For details, refer to Section 6 of P2526 ADT User Manual regarding Application Data Verification.	

Table C–1. Safety-Related Application Checklist (Cont.)

Safety-Related Application Condition Number	Responsible Personnel	Safety Related Application Conditions / Action	Evidence for Implementation
SRAC.2	Application Design Installation Maintenance	The installation, testing, and validation process must ensure that the microWIU is loaded with the correct application logic.	
SRAC.3	Application Design Operator	Design of user interfaces shall restrict access to authorized personnel, especially to those functions that can affect safety.	
SRAC.4	Application Design Installation Maintenance	The configuration control and verification and validation processes must ensure that the microWIU is correctly configured.	
SRAC.5	Installation Maintenance	Personnel must be trained and training must be sufficient to convey understanding of safety requirements and precautions.	
SRAC.6	Application Design	PTC subsystems receiving microWIU messages must enter and/or maintain a safe state/operation in the presence of communications overload from the microWIU.	

Table C–1. Safety-Related Application Checklist (Cont.)

Safety-Related Application Condition Number	Responsible Personnel	Safety Related Application Conditions / Action	Evidence for Implementation
SRAC.7	Application Design Installation Maintenance	Application design process must ensure proper interface specifications (e.g. Implement project level Interface Hazard Analysis). Interface requirements to uWIU must be unambiguously specified according to Product characteristics. Input constraint that a non-permissive signal must be less than 3.4V - 10.2mA (considering component tolerances as well as the worst case combination of failures). Personnel must be trained and qualified, in accordance with the product installation or maintenance manuals before installing or servicing microWIU equipment. Prior to installation, validation testing must confirm that all application logic is correct.	
SRAC.8	Application Design Installation Operation Maintenance	Processing of ACSES output messages when in the Shadow mode must “vitally” ensure that if the message is inadvertently transmitted to the wrong port (i.e., the ACSES network port vs the specified shadow mode port), then the message will NOT be acceptable by the ACSES OBC (i.e., it will fail the protocol checks; such as an incorrect 72-bit CRC).	
SRAC.9	Application Design	The verification process using the Application Data Verifier must be performed to ensure Vital application data structures are correct. Prior to installation, validation testing must confirm that all application logic is correct.	

Table C–1. Safety-Related Application Checklist (Cont.)

Safety-Related Application Condition Number	Responsible Personnel	Safety Related Application Conditions / Action	Evidence for Implementation
SRAC.10	Application Design	The safety level provided by the ACSES and/or ITC protocol(s) must be considered for the application. ITC and ACSES protocols must protect the Vital information and the OBC must respond safely to receipt of any messages not meeting protocol and/or expected requirements (e.g. out of sequence, unexpected, same time stamp).	
SRAC.11	Application Design Installation Maintenance	Railroad correspondence (validation) testing must be conducted to ensure that microWIU configuration and physical connections agree with railroad track conditions. The verification and validation process must ensure that the microWIU is configured correctly.	
SRAC.12	Application Design Installation	The installation, testing, and validation process must ensure that the microWIU is loaded with the correct application logic.	
SRAC.12a	Application Design Installation Operation & Maintenance	Railroad must manage Login and Password for authorized staff. Remote access via TCP/IP connection is secured by SSL and controlled by Login and Password.	

Table C–1. Safety-Related Application Checklist (Cont.)

Safety-Related Application Condition Number	Responsible Personnel	Safety Related Application Conditions / Action	Evidence for Implementation
SRAC.13	Installation Maintenance	Personnel must be trained and qualified, in accordance with the product installation or maintenance manuals before installing or servicing microWIU equipment. The input cables and connectors are to be keyed and the connectors are clearly labeled. Appropriate field testing must be done after installation/maintenance is performed.	
SRAC.14	Alstom Application Design Installation	Use of unique physical keying shall be used to ensure the correct Baseline hardware and software is installed. Personnel must be trained and qualified, in accordance with the product installation or maintenance manuals before installing or servicing microWIU equipment. Prior to installation, validation testing must confirm that all application logic is correct.	
SRAC.15	Installation Operation Maintenance	Equipment access doors must be locked. The microWIU equipment must only be serviced by authorized and qualified personnel according to product installation or maintenance manuals. All equipment access to be protected by user access procedures that are consistent with cyber-security practice throughout the industry. Critical cables connections to be keyed.	

Table C–1. Safety-Related Application Checklist (Cont.)

Safety-Related Application Condition Number	Responsible Personnel	Safety Related Application Conditions / Action	Evidence for Implementation
SRAC.16	Maintenance	Training of railroad staff shall be required before servicing any microWIU. Training & Maintenance records will be maintained to assure proper maintenance.	
SRAC.17	Maintenance	Maintenance personnel must be trained and qualified before servicing PTC equipment. Proper operation of PTC must be verified by field test after repair and before use. When boards are replaced, record the source/nature of the fault, part number, serial number, location for the component that is removed. Boards affecting safety shall be keyed. Clarification: microWIU is designed as a Line Replaceable Unit (LRU) i.e., Boards cannot be replaced/removed on site.	
SRAC.18	Application Design	On-board equipment must fail safely if data from microWIU is not provided or delayed.	
SRAC.19	Operation Maintenance	Maintainers must review microWIU error logs and repair or remove from service a microWIU reporting Heath-Sync-Lost or Fatal-Error type error(s) within 4 days. Any operational impact that may be due to the microWIU (such as, On-Board unit fails to receive message from microWIU or On-board unit receives invalid messages from the microWIU) must be reported to maintenance department daily by railroad personnel (i.e. by Locomotive engineers or trackside workers). Maintainers must repair or remove from service any microWIU reporting the Heath-Sync-Lost or Fatal-Error type error(s type error(s) or any microWIU reported as potentially impacting operations within four days.	
SRAC.20	Operation Maintenance	For microWIUs operating in ACSES mode, the maintainers must follow the periodic maintenance recommendation as described in the Operations and Maintenance Manual.	

Table C–1. Safety-Related Application Checklist (Cont.)

Safety-Related Application Condition Number	Responsible Personnel	Safety Related Application Conditions / Action	Evidence for Implementation
SRAC.21	Application Design Installation Maintenance	The microWIU system must be installed in a way that eliminates or reduces the risk of external influences affecting the voltages present on the microWIU's Vital inputs.	
SRAC.22	Application Design Installation Maintenance	Wayside equipment serving as Vital inputs to a microWIU must itself be Vital.	
SRAC.23	Application Design Installation	The procedure for configuring and installing microWIU units must ensure correlation between the configuration and the site of installation.	
SRAC.24	Application Design Operation	Equipment that receives ACSES/ITC messages from microWIU units must safely handle situations in which messages from the microWIU are transmitted with abnormal frequency.	
SRAC.25	Application Design Operation	Equipment that receives ACSES/ITC messages must safely handle the reception of outdated messages, as revealed by the messages' timestamps.	

Table C–1. Safety-Related Application Checklist (Cont.)

Safety-Related Application Condition Number	Responsible Personnel	Safety Related Application Conditions / Action	Evidence for Implementation
SRAC.26	Application Design Operation	Equipment that receives ACSES/ITC messages must safely handle the reception of messages that are not the type for which the microWIU is configured.	
SRAC.27	Application Design Installation Operation Maintenance	The microWIU design is to be tested for safe and correct performance in the presence of standard limits of external interference, as specified in the Hardware Requirements Specification AREMA compliant.	
SRAC.28	N/A	Cancelled.	
SRAC.29	Application Design Installation Operation Maintenance	The EMI sensitivity of equipment external to the microWIU is outside the scope of this product-level analysis.	
SRAC.30	Application Design Installation	All interfaces between the microWIU and other equipment with which it is compatible must be tested and their performance must be verified.	

Table C–1. Safety-Related Application Checklist (Cont.)

Safety-Related Application Condition Number	Responsible Personnel	Safety Related Application Conditions / Action	Evidence for Implementation
SRAC.31	Application Design	The end-user application of the microWIU's non-Vital outputs is outside the scope of this product-level analysis.	
SRAC.32	Application Design Installation	microWIU Baseline 4 and 5 units are compatible with external equipment with valid FLASHING state outputs. All interfaces between the microWIU and other equipment which could result in spurious FLASHING must be analyzed and tested and their performance must be verified.	
RAC.33*	Application Design	The on-site robustness of the CAN bus protocol is outside the scope of this product-level analysis.	
SRAC.34	Application Design	Slave identification information, contained within a microWIU's configuration data, must be correct.	
SRAC.35	Application Design	The input state requirements for generating particular ACSES messages must be verified at the application level and measures must be taken to confirm that the microWIU's ADS contents are consistent with the application requirements.	
SRAC.36	Installation	Master/slave network connections must be installed correctly and verified.	
SRAC.37	Application Design	The microWIU's handling of ACSES Timestamp message field must be considered by the application.	
SRAC.38	Application Design	The microWIU's handling of ACSES Train ID message field must be considered by the application.	
SRAC.39	Application Design	The input state requirements for generating ITC messages must be verified at the application level.	
SRAC.40	Application Design	The Boolean logic functions that are a part of the construction of ITC messages must be verified at the application level and measures must be taken to confirm that the microWIU's ADS contents are consistent with the application requirements.	

Table C–1. Safety-Related Application Checklist (Cont.)

Safety-Related Application Condition Number	**Responsible Personnel**	**Safety Related Application Conditions / Action**	**Evidence for Implementation**
SRAC.41	Application Design Installation Maintenance	Formal application engineer training shall explain proper selection and use of VSOE2 including message configuration. The verification and validation process (supported by the ADV tool) must ensure that the uWIU and VPI are programmed with the correct application logic and is correctly configured. Note: uWIU and VPI shall not be viewed as two independent products. The verification and validation process must ensure the coherency and the compatibility between uWIU and VPI.	
SRAC.42	Application Design Installation Maintenance	The Ethernet network shall be maintained as a private and dedicated communications network for Signaling to prevent malicious action.	

* Reliability Application Condition, not Safety-related

FOR QUESTIONS AND INQUIRIES, CONTACT CUSTOMER SERVICE AT
1-800-717-4477
OR
WWW.ALSTOMSIGNALINGSOLUTIONS.COM

ALSTOM SIGNALING INC.
1025 JOHN STREET
WEST HENRIETTA, NY 14586